Notes for Algebraic Structures

Spring 2016

Transcribed by Jacob Van Buren
(jvanbure@andrew.cmu.edu)

Notes for Algebraic Structures, taught Spring 2016 at Carnegie Mellon University, by Professor Clinton Conley.

Administrativia

Instructor. Clinton Conley (clintonc@andrew.cmu.edu), WEH 7121
http://www.math.cmu.edu/~clintonc/

Grading. 20% HW, 20% $\times$ 2 midterms, 40% Final

Homework. Wednesday-Wednesday. Graded for completeness, one starred problem for which no collaboration of any type is allowed.
Most homework out of textbook ("D&F").

Contents

The Integers

Lecture 1 (2016–01–11).

Notation. $\mathbb{N} := \{1, 2, 3, \ldots\}$ in this class.

Properties: Order, other things. Least element in a set S: $x \in S$ s.t. $\forall y \in S, x \leq y$
Addition $(\mathbb{Z}, +)$:

- Associativity $(x + y) + z = x + (y + z)$
- Identity $x + 0 = 0 + x = 0$
- Inversion $x + (-x) = (-x) + x = 0$
- Commutativity $x + y = y + x$

Multiplication $(\mathbb{Z}, +, \cdot)$:

- Associative
- Distributive
- Identity ("1")

Integer division: Assume x an integer and $y \in \mathbb{Z}^+$ then $\exists! d \in \mathbb{Z}, \exists! r \in \mathbb{Z} : 0 \leq r < y, x = d \cdot y + r$

Definition 1. $y|x$ "y divides x" iff $\exists d \in \mathbb{Z} : x = d \cdot y$.

E.g. $3\,|\,9, 4 \nmid 7$.

Definition 2. d is a GCD of x and y if

- $d\,|\,x, d\,|\,y$
- If $c\,|\,x$ and $c\,|\,y$ then $c\,|\,d$

Lecture 2 (2016–01–13).

Definition 3. Given $a, b \in \mathbb{Z}$, denote by $\mathbb{Z}(a, b)$ the set $\{ax + by | x, y \in \mathbb{Z}\}$.

Theorem 4 (Euclid, Bezout)**.** *Suppose $a, b \in \mathbb{Z}$ are nonzero and let d be the smallest positive element of $\mathbb{Z}(a, b)$, then d is the unique positive GCD of a and b.*

Proof. d is a GCD of a, b

(1) (Existence of positive GCD)
   (a) By integer division, $\exists q \in \mathbb{Z}, \exists r \in \mathbb{Z}$ with $0 \leq r < d$ such that $a = qd + r$. If $r = 0$ then $d|a$, so done. Otherwise, suppose $0 < r < d$, so $r = a - qd$ since $d \in \mathbb{Z}(a, b)$, we may fix x, y st $d = ax + by$, meaning $r = a - q(ax + by) = a(1 - qx) + b(-qy)$, so $r \in \mathbb{Z}(a, b)$, meaning d was not the minimal positive element in $\mathbb{Z}(a, b)$, RAA. Thus, $d\,|\,a$
   (b) Homework: If $c\,|\,a$ and $c\,|\,b$ then $c\,|\,(ax + by)$ for all $x, y \in \mathbb{Z}$ Hence $c\,|\,d$

(2) (Uniqueness of positive GCD) Suppose d_1, d_2 are both positive GCDs of a and b. $d_1 | d_2$ and $d_2 | d_1$ as they are both GCDs. i.e., $\exists m, n \in \mathbb{Z}$ such that $d_2 = md_1$ and $d_1 = nd_2$. As $\text{sgn}(d_1) = \text{sgn}(d_2)$, $m \geq 0$ and $n \geq 0$. As $d_1 = mnd_1$, $m = n = 1$. Thus $d_1 = d_2$.

□

Definition 5. Relatively prime $\iff$ $\gcd(a, b) = 1$

Theorem 6. *If p is prime, $a, b \in \mathbb{Z}$ are nonzero, and $p | (ab)$, then $p | a$ or $p | b$.*

Proof. Consider $d = \gcd(p, a)$. Since $d | p$, we know $d = p$ or $d = 1$.

If $d = p$: By def of GCD, $d | p$ and $d | a$ i.e. $p | p$ and $p | a$ so we're done.
If $d = 1$: Fix integers x and y such that $px + ay = 1$. $b = p(xb) + (ab)y$ as $p | p(xb)$ and $p | \underbrace{(ab)}_{\uparrow} y$, $p | b$.

□

Theorem 7 (Unique Prime Factorization)**.** *Suppose that $a > 1$ an integer, $m, n \geq 1$ and $p_1 \leq p_2 \leq \ldots \leq p_m, q_1 \leq q_2 \leq \ldots \leq q_m$ are positive primes.*

Then $m = n$ and $p_i = q_i$ for all i.

Proof. By induction, it suffices to show $p_1 = q_1$. Suppose not. WLOG, assume $p_1 < q_1$. We know that $p_1 | a$ (as $p_1 | q_1 q_2 \ldots q_n$) Hence, $\exists i \leq n$ such that $p_i | q_i$. since p_i and q_i prime, $p_1 = q_i$. However, $p_1 < q_1 \leq q_i = p_1$ so $p_1 < p_2$ contradiction.
Hence $p_1 = q_1$ so by induction, we're done. □

Lecture 3 (2016–01–15).

Teaser: Construct numbers of the form $a + b\sqrt{-5}$ with $a, b \in \mathbb{Z}$.
Notion of addition still exists: (similar to complex numbers, coefficients remain integers) Same with multiplication
Among these "numbers", 2 is irreducible. But, 2 is not prime, as $2 \nmid (1+\sqrt{-5})$ and $2 \nmid (1+\sqrt{-5})$, but $2 | \underbrace{(1 + \sqrt{-5})(1 - \sqrt{-5})}_{=6=2\cdot 3}$.

The Integers (mod n)

For today, $n > 0$.

Definition 8. For $a, b \in \mathbb{Z}$ we say $a \equiv b \pmod{n}$ iff $n \,|\, (b - a)$.

$\equiv$ is an *equivalence relation*

- Reflexivity: $a \equiv a$
- Symmetry: $a \equiv b \iff b \equiv a$
- Transitivity: $a \equiv b \wedge b \equiv c \implies a \equiv c$

  Proof. We know that $a \equiv b$ and $b \equiv c$, i.e. $n \,|\, (b - a)$ and $n \,|\, (c - b)$ We want $a \equiv c$, i.e., $n \,|\, (c - a)$

$$c - a = c + (-b + b) - a = \underbrace{(c - b) + (b - a)}_{n \text{ divides these}}$$

  □

Definition 9. Denote by $\overline{a}$ or $[a]_n$ the equivalence class of a with respect to $\equiv \pmod{n}$ (I.e., The set $\{b \in \mathbb{Z} : a \equiv b \pmod{n}\} = \overline{\{a + kn : k \in \mathbb{Z}\}}$).

Example. If $n = 2$, there are 2 equivalence classes:
$\overline{0} = \{\ldots, -4, -2, 0, 2, 4, \ldots\} = \overline{2} = \overline{-36}$
$\overline{1} = \{\ldots, -3, -1, 1, 3, \ldots\}$

Definition 10. Denote by $\mathbb{Z}/n\mathbb{Z}$ the collection of all $\equiv \pmod{n}$ equivalence classes.

E.g. $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$
"Define" addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$ as follows:

$$\overline{a} + \overline{b} = \overline{a + b}$$
$$\overline{a} \cdot \overline{b} = \overline{ab}$$

Makes sense, but we need to check that this definition makes any sense at all (make sure it's *well-defined*). Specifically, we need to make sure that the results of these operations doesn't depend on the representatives of the equivalence classes we chose (e.g. check that $\overline{x} + \overline{z} \equiv \overline{y} + \overline{z}$ if $x \equiv y$).
For brevity, we just show addition.

Theorem 11. *$+$ and $\cdot$ are well-defined on $\mathbb{Z}/n\mathbb{Z}$*

Proof. (of $\cdot$) Assume that $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ and $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$.
Then, we want to show that $a_1 b_1 \equiv a_2 b_2 \pmod{n}$.
We know: $n \,|\, (a_2 - a_1)$ and $n \,|\, (b_2 - b_1)$.

We want: $n \mid (a_2b_2 - a_1b_1)$.

$$\begin{aligned} a_2b_2 - a_1b_1 &= a_2b_2 + (-a_1b_2 + a_1b_2) - a_1b_1 \\ &= (a_2b_2 - a_1b_2) + (a_1b_2 - a_1b_1) \\ &= \underbrace{(a_2 - a_1)b_2 + a_1(b_2 - b_1)}_{n \text{ divides these}} \end{aligned}$$

So, $n \mid (a_2b_2 - a_1b_1)$ as desired □

Remark: This is a special case of a "quotient construction," in which you start with a set and an equivalence relation on it and operations on the set that "respect" the equivalence relations (i.e. equivalent inputs yield equivalent outputs)
More notes: Multiplicative inverses are uncommon in the integers (only for 1 and -1). However, it's "more prevalent" in $\mathbb{Z}/n\mathbb{Z}$ in the following sense:

Theorem 12. *Suppose $n > 0$ is an integer, $a \in \mathbb{Z}$ such that $\gcd(n, a) = 1$ (they're coprime). Then there is $b \in \mathbb{Z}$ such that $ab = 1 \pmod{n}$ (alternatively, $\overline{a} \cdot \overline{b} = \overline{1}$)*

Proof. Use Bézout's identity (from last lecture) Take integers x, y such that $nx + ay = \gcd(a, n) = 1$. Then, $nx = 1 - ay$, so $n \mid (1 - ay)$, so $1 \equiv ay \pmod{n}$, Choose $b = y$ and we're done ($\overline{a}\overline{b} \equiv \overline{1}$). □

Groups

Definition 13. We say that $*$ is a binary operation on some set X if it is a function $* : X \times X \to X$. (That is, $*$ accepts two (ordered) inputs from X and it outputs one element of X.)

Remark: usually write $a * b$ for the output of $*$ on the input (a, b).

Definition 14. A group is a set G with a binary operation $*$ (often abbreviated $(G, *)$) satisfying the following 3 axioms.

i. Associativity: $\forall a, b, c \in G : (a * b) * c = a * (b * c)$
ii. Identity: There is some $e \in G$ such that $\forall a \in G : a * e = e * a = a$
iii. Inversion: $\forall a \in G(\exists b \in G(a * b = b * a = e))$ (where e is as described in ii)

Lecture 4 (2016–01–20).

Recall the definition of a group.

Definition 15. $(G, *)$ is an abelian (commutative) group if it is a group and

iv. $(G, *)$ is commutative $(\forall x, y \in G : x * y = y * x)$

Let $(G, *)$ be an arbitrary but fixed group.

Proposition 16. *There is a unique identity element.*

Proof. Suppose e and f both satisfy the second group property. we compute $e * f$ in two ways. $e * f = f$ and $e * f = e$, so by transitivity, $e = f$. □

Proposition 17. *If $a \in G$, a has a unique inverse.*

Proof. Suppose that b and c are both inverses for a, $b * a = e$, $a * c = e$. Then,

$$b = b * e = b * (a * c) = (b * a) * c = e * c = c$$

□

Notational Conventions.

- We will often just call a group G instead of $(G, *)$
- We abbreviate multiplication $(x * y)$ as $x \cdot y$ or just xy
- We will often write xyz for $(x * y) * z$ (due to associativity)
- When working with $(\mathbb{Z}, +)$, we'll just use $+$
- We'll denote the (unique) identity of G by 1 or by e.
- We'll denote the inverse of x by x^{-1}
- Given an integer exponent $n \in \mathbb{Z}$ and $x \in G$, define

$$x^n = \begin{cases} \prod_{i=1}^{n} x, & \text{if } n > 0 \\ e, & \text{if } n = 0 \\ \prod_{i=1}^{-n} (x^{-1}), & \text{if } n < 0 \end{cases}$$

Group Examples. "Definition:" $\mathbb{Q} = \left\{ \frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{Z}^+ \right\}$

(1) $(\mathbb{Z}, +)$ is an abelian group
(2) $(\mathbb{Z}, \times)$ is not a group
    Why? 2 has no inverse in $\mathbb{Z}$. $(\nexists x \in \mathbb{Z} : (2x = 1))$
(3) $(\mathbb{Q}, +)$ is an abelian group
(4) $(\mathbb{Q}, \times)$ is not a group (0 has no inverse)
(5) $(\mathbb{Q} \setminus \{0\}, \times)$ is an abelian group.
(6) $\mathrm{GL}(n)$ is the set of matrices $A_{n\times n}$ for which $\det A_{n\times n} \neq 0$
(7) The set G of 2×2 matrices with determinant 1, along with matrix multiplication, is a group. Called the "special linear group."

Closure:

$$\det\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} e & f \\ g & h \end{smallmatrix}\right)\right) = (bc - ad)(fg - eh) = 1$$

i. Associativity: proof left for the reader.
ii. Identity: $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$
iii. Given $a = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, take $a^{-1} = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$, which you can verify is still in G.

The group is *not* abelian. Take $a = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), b = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$. Verify that $ab \neq ba$

(8) Suppose that $X \neq \emptyset$ is some set, and denote by S_X the set of bijections $f : X \to X$. Then $(S_X, \circ)$ is a group, where $\circ$ is function composition. $((f \circ g)$ is the function $x \mapsto f(g(x)).)$
    Identity is $x \mapsto x$. Inversion $f^{-1} = f^{-1}$.

Symmetric Groups

Lecture 5 (2016–01–25).

Recall: if X is a set then S_X is the group of bijections on it.

Definition 18. S_X (or Sym_X) is called the symmetric group on X.

Note: $\circ$ is associative because $(f \circ g) \circ h$ is

$$x \overset{\mathsf{h}}{\mapsto} (x) \overset{\mathsf{g}}{\mapsto} g(h(x)) \overset{\mathsf{f}}{\mapsto} f(g(h(x)))$$

Note: if $X = \{1, \ldots, n\}$, then we usually write S_n instead of $S_{\{1,\ldots,n\}}$. (Sometimes called symmetric group of degree n.)

Let's examine S_3:

elt.	1	2	3
e	1	2	3
a	1	3	2
b	2	1	3
c	2	3	1
d	3	1	2
f	3	2	1

The group has $6 = 3!$ elements.

Lets compute ab and ba

$ab = a \circ b$, looking it up in the table gives $ab = d$ and $ba = c$.

In particular, S_3 is not abelian.

Definition 19. A cycle is a permutation σ of the following form:

There is a sequence $x_1, x_2, \ldots, x_m$ of finitely many (distinct) elements of $\{1, 2, \ldots, n\}$ such that $\sigma(x_{i-1}) = x_i$, $\sigma(x_m) = x_1$, and $\sigma(y) = y$, for $y \notin \{x_1, \ldots, x_m\}$.

We call m the length of the cycle.

Ex. In S_3, $d = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix}\right)$ is a cycle of length 3, with $x_1 = 1, x_2 = 3, x_3 = 2$.

Ex. In S_3, $a = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right)$ is a cycle of length 2, with $x_1 = 2, x_2 = 3$.

Notation. Given a cycle, we can efficiently denote it by $(x_1\, x_2\, x_3\, \ldots\, x_m)$.

Example. In S_3, $a = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right)$ would be written as (1 3 2).

Let's work in S_5.

$\varphi := \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{smallmatrix}\right)$ is not a cycle, but it is the "superposition" of two cycles (1 3) and (2 4 5). Thus, we may write $\varphi =$(1 3) $\circ$ (2 4 5), or (2 4 5)(1 3).

Theorem 20. *Every permutation in S_n may be written as the product of "disjoint" cycles. (The identity is the empty product).*

Proof. Sketch: If you have e then you're done trivially.

Otherwise, fix the least element x of $\{1, \ldots, n\}$ "moved" by σ (i.e. $\sigma(x) \neq x$). Look at $x, \sigma(x), \sigma^2(x), \ldots, \sigma^m(x) = \sigma^n(x)$, $n < m$. So, as σ is invertible, $\sigma^{m-n}(x) = x$, so x is part of a cycle. □

Theorem 21. *Cycles can be written as a product of transpositions.*

General propositions on inversion in groups. Let G be a group, and let $a, b, x \in G$ be arbitrary.

- $(a^{-1})^{-1} = a$

  Proof. Show that a is the inverse of a^{-1}. Follows from group axiom. □

- $(ab)^1 = b^{-1}a^{-1}$

  Proof. $(ab)(b^{-1}a^{-1}) = (a(bb^{-1}))a^{-1} = (ae)a^{-1} = aa^{-1} = e$. Similarly, this works when we multiply from the other side. □

Lecture 6 (2016–01–27).

Definition 22. The cardinality (or order) of a group G is the number of elements in it, denoted by $|G|$.

Example.

- $|\mathbb{Z}| = \infty (= \aleph_0)$
- $|(\mathbb{Z}/5\mathbb{Z})| = 5$
- $|S_4| = 4! = 24$

Definition 23. Given a group G and $x \in G$, the order of x is the smallest integer $n > 0$ such that $x^n = e$. If no such n exists, we say the order is ∞.
We denote by $|x|$ the order of x.

Example. In $(\mathbb{Z}, +)$: $|0| = 1$, $|5| = \infty$.
In S_5: $|(1\ 3)| = 2$, $|(2\ 4\ 5)| = 3$, $|(1\ 3)(2\ 4\ 5)| = 6$.

Proposition 24. *If G is a* finite *group, every $x \in G$ has finite order. Moreover, $|x| \leq |G|$.*

Proof. Say $|G| = k$. Consider the sequence $x^0, x^1, x^2, \ldots, x^k$. There are $k + 1$ items in the sequence. So $\exists m < n$ such that $x^m = x^n$. $x^{n-m} = x^n x^{-m} = x^m x^{-m} = e$. As $0 < n - m \leq k$, it follows that $|x| \leq n - m \leq |G|$. □

Subgroups

Definition 25. Suppose $(G, *)$ is a group and $H \subseteq G$ some subset of G. We say H is a subgroup of G, written $H \leq G$ if $(H, *)$ happens to be a group, i.e., the following properties hold:

$*$ is a associative binary operator on H (i.e., it's closed) with inverses and an identity element.

Example.

- $\mathbb{Z} \leq \mathbb{Q}$ (under addition)
- Even integers $\leq \mathbb{Z}$ (under addition)
- $n\mathbb{Z} \leq \mathbb{Z}$, where $n\mathbb{Z} := \{nx : x \in \mathbb{Z}\}$
  Aside: every subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$
- $\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \leq S_4$.

Proposition 26. *(Homework): $H \leq G$ iff*
(a) $H \neq \emptyset$ (nonempty)
(b) $\forall x, y \in H (xy \in H)$ (closed under product)
(c) $\forall x \in H (x^{-1} \in H)$ (closed under inverses)

Proposition 27. *Suppose G is a* finite *group. Then $H \leq G$ iff $H \neq \emptyset$ and $\forall x, y \in H : xy \in H$.*

Proof. We show that for $H \subseteq G$ (a) and (b) $\implies$ (c) (letters from proposition (26))
Fix $x \in H$. Since G is finite, $|x|$ is finite (in G). Say $|x| = n > 0$ $x^n = \underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ times}} = e_G$.
Hence, $e_G \in H$.
Examine x^{n-1}.

$$x^{n-1} = \begin{cases} x^0 = e & \text{if } n = 1 \\ \underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ times}} & \text{if } n > 1 \end{cases}$$

But $x^{n-1} = x^{-1}$, since $x^{n-1}x = x^n = xx^{n-1} = e$. Thus, (c) holds for H. □

Remark. $\mathbb{N} = \{0, 1, \ldots\} \subseteq \mathbb{Z}$, but $\mathbb{N} \not\leq \mathbb{Z}$, despite satisfying (a) and (b).

(Left) Coset equivalence

Suppose G is a group and $H \leq G$ is a subgroup of G.

Definition 28. We say $x \sim y \pmod{H}$ if $x^{-1}y \in H$.

Proposition 29. $\sim \pmod{H}$ *is an equivalence relation.*

Proof.

- Reflexivity ($x \sim x$):
  $x^{-1}x = e \in H$, so $x \sim x$.
- Symmetry ($x \sim y \implies y \sim x$):
  We know $x^{-1}y \in H$. H is closed under inversion, so $H \ni (x^{-1}y)^{-1} = (y^{-1}(x^{-1})^{-1}) = (y^{-1}x)$. Thus, $y \sim x$.
- Transitivity ($(x \sim y) \wedge (y \sim z) \implies (x \sim z)$):
  We know $x^{-1}y \in H$ and $y^{-1}z \in H$.
  Thus, $H \ni (x^{-1}y)(y^{-1}z) = x^{-1}ez = x^{-1}z$, so $x \sim z$.

□

Lecture 7 (2016–01–29).

G is a group. $H \leq G$ a fixed subgroup of G.
Given $x, y \in G$, $x \sim y \pmod{H}$ iff

$$x^{-1}y \in H.$$

Last time: we showed it was an equivalence relation.
What are the equivalence classes of $\sim \pmod{H}$? We examine

$$\begin{aligned}
[x] &= \{y \in G : x \sim y \pmod{H}\} \\
&= \{y \in G : x^{-1}y \in H\} \\
&= \{y \in G : \exists h \in H(x^{-1}y = h)\} \\
&= \{y \in G : \exists h \in H(x(x^{-1}y) = xh)\} \\
&= \{y \in G : \exists h \in H(y = xh)\}
\end{aligned}$$

So, $[x]$ is exactly the set

$$\{xh : h \in H\}.$$

Notation. We write xH to abbreviate the set $\{xh : h \in H\}$.

Definition 30. The equivalence class xH is called the (left) coset of x with respect to H.

Notation. The cyclic subgroup of x is denoted by $\langle x \rangle$.

Examples:

- $G = (\mathbb{Z}, +)$, $H = n\mathbb{Z}$ = multiples of n. So $H \leq G$. For $x \in \mathbb{Z}$, its coset is $\overline{x} = \{x + h : h \in n\mathbb{Z}\} = \{x + nk : k \in \mathbb{Z}\}$
- $G = S_3 = \{e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$ Take $H = \{e, (1\ 2\ 3), (1\ 3\ 2)\} \leq S_3$ (the cyclic subgroup of (1 2 3)).

  So what are the cosets? $eH = \{eh : h \in H\} = \{h : h \in H\} = H$. (In general, eH is always just H). (Even more generally, $xH = H$ whenever $x \in H$.)

  Another coset is $(1\ 2)H$. Just compute $(1\ 2)h$ for each $h \in H$. Thus

$$(1\ 2)H = \left\{ \begin{array}{lll} (1\ 2) & e & = (1\ 2) \\ (1\ 2) & (1\ 2\ 3) & = (2\ 3) \\ (1\ 2) & (1\ 3\ 2) & = (1\ 3) \end{array} \right\} = \{(1\ 2), (2\ 3), (1\ 3)\}$$

  We note that $(1\ 2)H = (2\ 3)H = (1\ 3)H$, as each of those are in $(1\ 2)H$.
- $G = S_3$, $K = \langle (1\ 3) \rangle = \{e, (1\ 3)\} \leq G$. Analyze cosets mod K.

  Easy coset: $eK = K$.

  For the next coset, choose $(1\ 2\ 3)K$

$$(1\ 2\ 3)K = \left\{ \begin{array}{ll} (1\ 2\ 3)\ e & = (1\ 2\ 3) \\ (1\ 2\ 3)\ (1\ 3) & = (2\ 3) \end{array} \right\} = \{(1\ 2\ 3), (2\ 3)\}$$

  Next coset after that is $(1\ 2)K = \{(1\ 2), (1\ 3\ 2)\}$.

  We note that the equivalence classes mod K partition S_3, Although they are not all subgroups.

In the last two examples, it wasn't a coincidence that each coset was of the same cardinality.

Proposition 31. *Suppose G is a group, $H \leq G$, and $x \in G$. Then $|xH| = |H|$.*

Proof. We establish a bijection between H and xH.
Define $\varphi : H \to xH$, $\varphi(h) = xh$.

Claim (1). φ is surjective.

Proof. Suppose $y \in xH$.
By definition of xH, $\exists h \in H$ such that $y = xh$. So, $y = \varphi(h)$. □(C1)

Claim (2). φ is injective.

Proof. Suppose $h_1, h_2 \in H$ such that $\varphi(h_1) = \varphi(h_2)$.
By definition of φ, we have $xh_1 = xh_2$. Since G is a group, x has an inverse x^{-1}.
Thus, $x^{-1}(xh_1) = x^{-1}(xh_2) \implies h_1 = h_2$ as desired. □(C2)

Thus φ is a bijection, meaning $|xH| = |H|$ as desired. □(Prop.)

Theorem 32 (Lagrange's Theorem)**.** *Suppose that G is a finite group and $H \leq G$. Then $|H|$ divides $|G|$.*

Proof. Left coset equivalence partitions G into k equivalence classes of size $|H|$.
Thus $|G| = k|H|$, as desired. □

Corollary 33. *Suppose that G is a finite group and $x \in G$. Then $|x|$ divides $|G|$.*

Proof. Consider $\langle x \rangle$ (the cyclic subgroup generated by x). $\langle x \rangle = \{e, x, x^2, \ldots, x^{n-1}\}$, where $|x| = n$. $|\langle x \rangle| = n$. Hence $n = |x|$ divides $|G|$. □

Lecture 8 (2016–02–01).

We go to the previous lecture for examples.
Consider $G = S_3, H = \{e, (1\ 2\ 3), (1\ 3\ 2)\} \leq G$, $K = \langle (1\ 3) \rangle = \{e, (1\ 3)\} \leq G$.

Definition 34. If G is a group and $H \leq G$, denote by G/H (G "mod" H) the collection of (left) cosets of H in G.

Example.

(a) $n\mathbb{Z} \leq \mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$
(b) $S_3/H = \{eH, (1\ 2)H\}, \quad eH = H, \quad (1\ 2)H = \{(1\ 2), (2\ 3), (1\ 3)\}$
(c) $S_3/K = \{\{e, (1\ 3)\}, \{(1\ 2\ 3), 23\}, \{(1\ 2), (1\ 3\ 2)\}\}$

Normal Subgroups

Fundamental question: When is there "natural" group operation on G/H? Prototype: $\mathbb{Z}/n\mathbb{Z}$, $\overline{x} + \overline{y} = \overline{x+y}$.
Natural Attempt:

$$(g_1H)(g_2(H)) \stackrel{?}{=} (g_1g_2)H.$$

This works fine for (b) in the sense that if $g_1H = g_2H$ and $k_1H = k_2H$ then $(g_1k_1)H = (g_2k_2)H$ (verification left to reader).
But it *doesn't* work for (c). e and $(1\ 3)$ both represent eK. But they give *different* cosets after multiplication by $(1\ 2\ 3)$.

- $e(1\ 2\ 3) = (1\ 2\ 3)$
- $(1\ 3)(1\ 2\ 3) = (1\ 2)$.

In general, what would we need to have, in order to have multiplication in G/H be "well-defined?"
We want: $\underbrace{x_1 \sim x_2}_{x_1^{-1}x_2 = h \in H}$ and $\underbrace{y_1 \sim y_2}_{y_1^{-1}y_2 = k \in H} \implies x_1y_1 \sim x_2y_2$. Thus, we want $(x_1y_1)^{-1}(x_2y_2) \in H$.

$$(x_1y_1)^{-1}(x_2y_2) = (y_1^{-1}x_1^{-1})(x_2y_2) = y_1^{-1}(x_1^{-1}x_2)y_1k = \underbrace{y_1^{-1}hy_1}_{\in H}\underbrace{k}_{\in H} \in H$$

This expression motivates the definition of a normal subgroup

Definition 35. If G is a group, and $N \leq G$, we say N is normal if for all $n \in N$, and $g \in G$, we have $g^{-1}ng \in N$. We write this as $N \trianglelefteq G$.

Remark. For fixed $g \in G$, the map for $x \in G$

$$x \mapsto g^{-1}xg$$

is called conjugation by g.
Thus, N is normal if it is stable under all conjugation.

Theorem 36. *Let G a group $H \leq G$. Then the following are equivalent:*

(I) $(g_1H)(g_2H) = (g_1g_2)H$ is a well-defined group operation on G/H.
(II) $H \trianglelefteq G$.

(II) $\implies$ (I). $x_1^{-1}x_2 = h, y_1^{-1}y_2 = k$. (Exercise for the reader) $\square$

(I) $\implies$ *(II).* Suppose $h \in H$ and $g \in H$ want $g^{-1}hg \in H$.
Note: $e \sim h$ since $e^{-1}h = h \in H$.
By (I),we have $(eg)H = (eH)(gH) = (hH)(gH) = (hg)H$.
So, $gH = (hg)H$, meaning $g \sim hg$, so $g^{-1}hg \in H$. □(Thm)

Proposition 37. *If G is abelian, every subgroup is normal.*

Proof. Fix $H \leq G$, $h \in H$, $g \in G$. Then $g^{-1}hg = g^{-1}gh = h \in H$. □

Proposition 38. *$G \trianglelefteq G$ and $\{e\} \trianglelefteq G$.*

Proof. $g^{-1}hg \in G$ and $g^{-1}eg = g^{-1}g = e \in \{e\}$. □

Definition 39. For $A \subseteq G$, denote by $g^{-1}Ag$ the set $\{g^{-1}ag : a \in A\}$.
Called the conjugate of A by G.

Remark. Thus, N is normal iff $N \leq G$ and $\forall g \in G : g^{-1}Ng \subseteq N$.

Proposition 40. $N \trianglelefteq G \implies \forall g \in G : g^{-1}Ng = N$

Proof. Fix $n \in N$. we want $n \in g^{-1}Ng$. (This shows $N \subseteq g^{-1}Ng$.)
We know by $N \trianglelefteq G$ that $m = (g^{-1})^{-1}n(g^{-1}) \in N$. Then $m = gng^{-1}$.
Claim. $g^{-1}mg = n$
Proof. $g^{-1}(gng^{-1})g = \cancel{(g^{-1}g)}n\cancel{(g^{-1}g)} = n$ □(Claim)
□(Prop)

Homomorphisms

Definition 41. Suppose G, H are groups and $\varphi : G \to H$ is a function. We say φ is a homomorphism if $\forall g_1, g_2 \in G : \phi(g_1 *_G g_2) = \varphi(g_1) *_H \varphi(g_2)$.

Definition 42. Suppose $\varphi : G \to H$ is a homomorphism. The Kernel of ϕ is $\text{Ker}(\varphi) = \{g \in G : \varphi(g) = e_H\} = \varphi^{-1}(\{e_H\})$.

Proposition 43. *Suppose $\varphi : G \to H$ is a homomorphism between groups.*
Then $K = \text{Ker}(\varphi) \trianglelefteq G$.

Proof.

Claim (1). $K \neq \emptyset$. In fact, $e_G \in K$.

Proof. We know that e_G is the unique element of G such that $\forall g \in G(e_G g = g e_g = g)$.
So, $\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G) = \varphi(e_G)$ Multiplying both sides by $\varphi(e_G)^{-1} \in H$
So $\varphi(e_G) = e_H$. □(C1)

Claim (2). $\forall g \in G \varphi(g^{-1}) = (\varphi(g))^{-1}$

Proof. $\varphi(g^{-1})\varphi(g) = \varphi(gg^{-1}) = \varphi(e_G) = e_H$ By symmetry, $\varphi(g)\varphi(g^{-1}) = e_H$ □(C2)

□(Prop.)

Lecture 9 (2016–02–03).

Class Note

Midterm 1 is on Friday February 26th (in class)

Last time: showed that the kernel of a homomorphism is a subgroup.

Proposition 44. $K \trianglelefteq G$.

Proof. First we show $K \leq G$.

- $K \neq \emptyset$ as $e_G \in K$.
- $\forall g_1, g_2 \in K, g_1 g_2 \in K$:
  $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = e_H e_H = e_H$ So $g_1 g_2 \in K$
- $\forall g \in H, g^{-1} \in K$:
  $\varphi(g^{-1}) = (\varphi(g))^{-1} = e_H^{-1} = e_H$
  So $g^{-1} \in K$

Thus, $K \leq G$. Next, we prove. $\forall k \in K, \forall g \in G$:

$$\varphi(g^{-1}kg) = \varphi(g^{-1})\varphi(h)\varphi(g) = (\varphi(g))^{-1} e_H \varphi(g) = e_H$$

Hence $g^{-1}kg \in K$. □

Definition 45. If $\varphi : G \to H$ is a group homomorphism, and $h \in H$, the fiber above h is the set $\varphi^{-1}(\{h\})$.

Thus, $\mathrm{Ker}(\varphi)$ is the fiber above e_H.

Example.

- $\varphi(\mathbb{R}, +) \to (\mathbb{R}^+, \times)$, $\varphi(r) = \mathrm{e}^r$ φ is a homomorphism since $\varphi(r+s) = \mathrm{e}^{r+s} = \mathrm{e}^r\mathrm{e}^s = \varphi(r) \times \varphi(s)$
  $\mathrm{Ker}(\varphi) = \{r \in R : \varphi(r) = 1\} = \{0\}$.
  The fiber above $s \in \mathbb{R}^+$: $\varphi(r) = s \iff \mathrm{e}^r = s \iff r = \ln s$. Thus $\varphi^{-1}(\{s\}) = \{\ln s\}$.
- $\varphi : (\mathbb{C} \setminus \{0\}, \times) \to (\mathbb{R} \setminus \{0\}, \times)$, $\varphi(a + b\mathrm{i}) = a^2 + b^2$.
  φ is a homomorphism (verification left to the reader).
  $\mathrm{Ker}(\varphi) = \{a + b\mathrm{i} : \varphi(a + b\mathrm{i}) = 1\} = \{a + b\mathrm{i} : a^2 + b^2 = 1\}$, which is the unit circle in the complex plane.
  Fix $r \in \mathbb{R} \setminus \{0\}$, lets examine the fiber above r:
  $$\{a + b\mathrm{i} : a^2 + b^2 = r\} = \begin{cases} \emptyset & \text{if } r < 0 \\ \text{Circle of radius } \sqrt{r} & \text{if } r > 0 \end{cases}$$
- Start with a group G, normal $N \trianglelefteq G$. $\varphi : G \to G/N$, $\varphi(g) = gN$ is a homomorphism.

  Proof. $\varphi(g_1g_2) = (g_1g_2)N = (g_1N)(g_2N) = \varphi(g_1)\varphi(g_2)$ □

  $\mathrm{Ker}(\varphi) = \{g : \varphi(g) = eN\} = \{g : \varphi(g) = eN\} = N$.

This leads us to the realization that:

Proposition 46. *$N \trianglelefteq G \iff N = \mathrm{Ker}(\phi)$ for some homomorphism $\varphi : G \to H$, for any group H.*

Why do all fibers look alike?

Proposition 47. *If $\phi : G \to H$ is a group homomorphism and $h \in H$, then $\varphi^{-1}(\{h\})$ is either $\emptyset$ or gK for some $g \in G$, where $K = \mathrm{Ker}(\varphi)$*

Proof. If $\nexists g \in G$ such that $\varphi(g) = h$ then $\varphi^{-1}(\{h\}) = \emptyset$.
Else, fix some $g \in G$ such that $\varphi(g) = h$.
Claim (1). $gK \supseteq \varphi^{-1}(\{h\})$

Proof. Suppose $g' \in \varphi^{-1}(\{h\})$ (i.e. $\varphi(g') = h$). Want $g' \in gK$. So, $\varphi(gg'^{-1}) = \varphi(g)\varphi(g'^{-1}) = \varphi(g)\varphi(g')^{-1} = hh^{-1} = e_H$. Hence $gg'^{-1} \in K$, so $g' \sim g \pmod K$, so $g' \in gK$. □(C1)

Claim (2). $gK \subseteq \varphi^{-1}(\{h\})$

Proof. Suppose $g' \in gK$, want $\varphi(g') = h$. Fix $k \in K$ such that $g' = gk$. $\varphi(g') = \varphi(gk) = \varphi(g)\varphi(k) = he_H = h$. □(C2)

Thus, $gK = \varphi^{-1}(\{h\})$, as desired. □(Prop.)

Corollary 48. *If $\varphi : G \to H$ is a group homomorphism, the following are equal:*

- *φ is injective.*
- $\mathrm{Ker}(\varphi) = \{e_G\}$

Definition 49. A map $\varphi : G \to H$ between groups is an isomorphism if it is a bijective homomorphism. We often say $G \cong H$ if there exists an isomorphism $\phi : G \to H$.

Intuition: Isomorphic groups have the "same operation" on different sets.

Example. Let $G = \{a, b\}$ $\begin{array}{c|cc} & a & b \\ \hline a & a & b \\ b & b & a \end{array}$ Then, $G \cong \mathbb{Z}/2\mathbb{Z}$ via $\varphi : a \mapsto \overline{0}, b \mapsto \overline{1}$

We know $\varphi : G \to H$ is an isomorphism if it's a homomorphism, surjective, and $\operatorname{Ker}(\varphi) = \{e_G\}$.

Lecture 10 (2016–02–06).

Definition 50. If $\varphi : G \to H$ is a function, denote by $\operatorname{Im}(\varphi)$, or $\varphi(G)$, or $\varphi[G]$ the image of G, i.e., the set $\{h \in H, \exists g \in G : \varphi(g) = h\}$.

Exercise. Prove: If $\varphi : G \to H$ is a group homomorphism then $\varphi[G] \leq H$.

Theorem 51 (First Isomorphism Theorem)**.** *If $\varphi : G \to H$ is a group homomorphism, then $\varphi[G] \cong G/\operatorname{Ker}(\varphi)$.*

Proof. Abbreviate $I := \varphi[G], K := \operatorname{Ker}(\varphi)$. We know for $h \in I$: $\varphi^{-1}(\{h\}) \neq \emptyset$. Hence, $\varphi^{-1}(\{h\}) = gK$ for some $gK \in G/K$. Then, define $\psi : I \to G/K$. $\psi(h) = \varphi^{-1}(\{h\}) = gK$.

Claim. $\psi : I \to G/K$ is a group isomorphism.

Proof. We show that ψ is a bijective homomorphism in three parts:

(a) ψ is a homomorphism:
Fix $h_1, h_2 \in I$, want $\psi(h_1, h_2) = \psi(h_1)\psi(h_2)$. Fix g_1, g_2 such that $\varphi(g_1) = h_1, \varphi(g_2) = h_2$. Then $\varphi(g_1 g_2) = h_1 h_2$ by def of homomorphism. So, $\psi(h_1 h_2) = g_1 g_2 K = (g_1 K)(g_2 K) = \psi(h_1)\psi(h_2)$. □(a)

(b) ψ is a surjection:
Fix $gK \in G/K$. Want $h \in I$ with $\psi(h) = gK$ Want $h \in I$ with $\psi(h) = gK$. Choose $h \in \psi(g)$. Then by def, $g \in \varphi^{-1}(\{h\})$. Thus, $\psi(h) = \varphi^{-1}(\{h\}) = gK$. □(b)

(c) ψ is an injection:
As remarked, it suffices to show

$$\operatorname{Ker}(\psi) = \{h \in I : \psi(h) = \underbrace{e_G K}_{=e_{G/K}}\} = \{h \in I : \varphi^{-1}(\{h\})\} = \{h \in I : \varphi(e_G) = h\} = \{e_H\}$$

□(c)

□(Claim)

□(Thm)

Definition 52. A group G is cyclic if $\exists x \in G : \langle x \rangle = G$. (Where $\langle x \rangle = \{x^n : n \in \mathbb{Z}\}$.)

Proposition 53. *If G is a cyclic group, then $G \cong \mathbb{Z}$, or $G \cong (\mathbb{Z}/n\mathbb{Z})$ for some $n \in \mathbb{Z}$.*

Proof. As G is cyclic, take $x \in G$ such that $\langle x \rangle = G$. the map $\varphi : (\mathbb{Z}, +) \to G$, $\varphi(n) = x^n$. By hypothesis, $\langle x \rangle = G$. φ is surjective, so $\operatorname{Im}(\varphi) = G$. By first isomorphism theorem, $G \cong (\mathbb{Z}/\operatorname{Ker}(\varphi))$.
Assume $\nexists n > 0$ such that $x^n = 1_G$ (i.e., the order of x in G is infinite.) Then $\operatorname{Ker}(\varphi) = \{n \cdot x^n = e_G\} = \{0\}$. Also $\mathbb{Z}/\{0\} \cong \mathbb{Z}$ (proof left as exercise). Thus, $G \cong \mathbb{Z}$.

Otherwise, fix the least $n > 0$ such that $x^n = e_G$(so $n = |x|$).
Check (exercise): $\operatorname{Ker}(\varphi) = \{m \in \mathbb{Z} : x^m = e_G\} = n\mathbb{Z}$. Thus $G \cong \mathbb{Z}/\operatorname{Ker}(\varphi) = \mathbb{Z}/n\mathbb{Z}$. □

Corollary 54. *Suppose $p > 1$ is prime and G is a group with $|G| = p$. Then $G \cong (\mathbb{Z}/p\mathbb{Z})$.*

Proof. Fix any $x \in G$, $x \neq e^G$. $|x| \neq 1$. Additionally $|x|$ divides $|G|$. Thus $|x| = p$, as p is prime. Then $\langle x \rangle = G$. □

Our next big motivational question: Given $n \in \mathbb{N}$, can we "classify" (or list) all groups of cardinality n (up to $\cong$)?
What we know so far:

n	Groups:
0	None
1	{e}
2	$\mathbb{Z}/2\mathbb{Z}$
3	$\mathbb{Z}/3\mathbb{Z}$
4	$\mathbb{Z}/4\mathbb{Z}, \ldots$?
5	$\mathbb{Z}/5\mathbb{Z}$
6	$\mathbb{Z}/6\mathbb{Z}, \ldots$?

Definition 55. G, H are groups, build a group of the direct product of G and H, denoted $G \times H$ with underlying set $\{(g, h) : g \in G, h \in H\}$, and group operation $(g_1, h_1) \cdot (g_2, h_2) = ((g_1 \cdot_G g_2), (h_1 \cdot_H h_2))$

Proposition 56. *If $|G| = 2$ then $G \cong \mathbb{Z}/4\mathbb{Z}$ or $G \cong ((\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}))$*

Lecture 11 (2016–02–08).

Proposition 57. *Suppose G is a group. Then $G/\{e_G\} \cong G$ and $G/G \cong \{e_G\}$.*

Proof. Consider the homomorphism $\varphi : G \to G$ with $\varphi(g) = g$ $\operatorname{Ker}(\varphi) = \{g \in G : \varphi(g) = e_G\} = \{e_G\}$, and $\varphi[G] = G$.
Thus, the first isomorphism theorem states that $G/\operatorname{Ker}(G) \cong \varphi[G]$.
Next, consider the homomorphism $\psi : G \to G$, $\psi(g) = e_G$. Then $\operatorname{Ker}(\psi) = G$, $\operatorname{Im}(\psi) = \{e_G\}$.
By the first isomorphism theorem, $G/G \cong \{e_G\}$. □

Groups of cardinality 4.

Proposition 58. *If G is a group with $|G| = 4$ then $G \cong \mathbb{Z}/4\mathbb{Z}$ or $G \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$.*

We note that the above groups are not isomorphic because there is no element of order 4 in $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$.

Proof. Possible orders for elements are 1, 2, or 4.
Two cases:

(1) $\exists g \in G, |g| = 4$ then $G = \langle g \rangle$, so (as proved last time) $G \cong (\mathbb{Z}/4\mathbb{Z})$.
(2) $\nexists g \in G, |g| = 4$:
So $G = \{e_G, a, b, c\}$, meaning $|e_G| = 1$ and $|a| = |b| = |c| = 2$. So $\forall g \in G(g^2 = e_G)$. Hence G is abelian (Homework). What is ab? It's not e_G as $a^{-1} = a \neq b$. It's not a since $b \neq e_G$. It's not b since $a \neq e_G$. So $ab = c$. Thus we may write the multiplication table.
Verification that $G \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ is left to the reader.

□

Remark. More generally, if p prime and $|G| = p^2$ then $G \cong (\mathbb{Z}/p^2\mathbb{Z})$ or $G \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$.

Proposition 59. *Suppose G is a group and $|G| = 6$. Then $G \cong (\mathbb{Z}/6\mathbb{Z})$ or $G \cong S_3$.*

Proof. (Sketch)
If $\exists x \in G$ with $|x| = G$ then $G = \langle x \rangle \cong (\mathbb{Z}/6\mathbb{Z})$.
More subtly, if $\exists a, b \in G$ such that $|a| = 3$ and $|b| = 2$ and $ab = ba$ then $G \cong (\mathbb{Z}/6\mathbb{Z})$ (verification that $|ab| = 6$ left as an exercise to the reader).
WLOG, assume all non-identity elements have order 2 or 3.
Also, elements of order 3 come in pairs. $|x| = 3, |x^{-1}| = 3, x \neq x^{-1}$. So $|\{x : |x| = 3\}| \in \{0, 2, 4\}$ (as it must be even, and $|e_G| = 1 \neq 3$).
Possible order breakdowns: either (A): 1 2 2 2 2 2 2, (B): 1 2 2 2 3 3, or (C): 1 2 3 3 3 3.

Claim (1). (A) can't happen. Why? Assume otherwise, then $\forall x \in G(x^2 = e)$ so G is abelian, so $\{1, a, b, ab\}$ is a subgroup, but $4 \not| 6$. so by Lagrange's theorem, this cannot happen.

Claim (2). (C) also cannot happen. Why? Assume otherwise, then denote by x the unique element of order 2. Then, $\forall g \in G, g^{-1}xg$ also has order 2. as

$$g^{-1}xgg^{-1}xg = g^{-1}x^2g = g^{-1}g = e$$

Thus, $g^{-1}xg$ has order 2. $\forall g \in G$, $g^{-1}xg = x \implies xg = gx$, contradiction.

Claim (3). (B) forces $G \cong S_3$. Proof of this follows from brute force considering the multiplication table.

□(outline)

Group Actions

"Groups, like men, shall be judged by their actions." – Unknown

Definition 60. Suppose G is a group (not necessarily finite), and X is a set (also not necessarily finite). A group action of G on X is formally a function $a : G \times X \to X$ such that $\forall x \in X : a(e_G, x) = x$, and $\forall g, h \in G, x \in X : a(gh, x) = a(g, a(h, x))$.

Notation. We write actions like this: $G \curvearrowright X$ "G acts on X," and $g \cdot x := a(g, x)$.
The conditions then become $e_G \cdot x = x$ and $(gh) \cdot x = g \cdot (h \cdot x)$.

Equivalently, instead of thinking about an action as a function of $(G \times X) \to X$, you can view it as a ("curried") function of $G \to (X \to X)$.
Say $g \mapsto \sigma_g$ where $\sigma_g \cdot (X \to X)$ is defined by $\sigma_g(x) = g \cdot x = a(g, x)$.

Claim. $\forall g \in G, \sigma_g$ is a permutation of X.

Proof. $\sigma_g \circ \sigma_{g^{-1}} = \sigma_{g^{-1}} \circ \sigma_g = \sigma_{e_G} (= x \mapsto x)$.
Why?

$$\sigma_g \circ \sigma_{g^{-1}}(x) = g \cdot (g^{-1} \cdot x) = (gg^{-1}) \cdot x = e_G \cdot x = x = \sigma_{e_G}(x)$$

Thus, σ_g is a bijection. □

An action then induces a map $G \to S_X$, $g \mapsto \sigma_g$. Note that $\sigma_g \circ \sigma_h = \sigma_{gh}$.

Property 61. Actions of G on X correspond to homomorphisms $G \to S_X$.

Example. Of actions:

(1) $X = \{1, 2, \ldots, n\}, S_n \curvearrowright X$ The action is $\sigma \cdot x = \sigma(x)$.
    More generally, if $H \leq S_n$, we get an analogous action.
(2) Let G be the 2×2 invertible matrices over $\mathbb{R}$ under the operation of matrix multiplication.
    $G \curvearrowright \mathbb{R}^2$ (acts on the Euclidean plane) by applying the matrices' corresponding linear transformation to the vector in $\mathbb{R}^2$. (Verification left to the reader.)
(3) $G = (\mathbb{R}, +)$ X is a circle. $G \curvearrowright X$ r "rotates the circle r radians c.c.w."

Lecture 12 (2016–02–10).

Note: group actions can be either left actions or right actions. However, we will only talk about left actions in this course, so we will refer to them exclusively as "actions."
Alternate def $G \to S_X$.
Important special case: $X = G$, then $G \curvearrowright G$ (G acts on itself).
There are three main actions:

- $G \curvearrowright G$ by left multiplication. $\forall g \in G, x \in X (= G), g \cdot x = gx$.
- $G \curvearrowright G$ by right multiplication. $g, x \in G, g \cdot x = xg^{-1}$.
- $G \curvearrowright G$ by conjugation. $g \cdot x = gxg^{-1}$. Note that gxg^{-1} is simply x conjugated by g^{-1}, so it doesn't matter whether we write $g^{-1}xg$ or gxg^{-1}.

Theorem 62 (Cayley)**.** *Suppose G is a group. Then there is a set X and a subgroup $H \leq S_X$ such that $G \cong H$.*
Moreover, we can choose X to have cardinality $|G|$. (i.e., if $|G| = n$, we can find an isomorphic copy of G inside S_n.)

Proof. Take $X = G$ and consider the action $G \curvearrowright G$ by left multiplication ($g \cdot x = gx$).
This induces a homomorphism $\varphi : G \to S_G, \varphi(g) = \lambda_g$ where $\lambda_g(x) = gx$.

Claim. $\operatorname{Ker}(\varphi) = \{e_G\}$.

Proof (Claim): Suppose $g \in G$ such that $\varphi(g) = e \in S_G$. so $\lambda_g = e$.
In particular, $e_G = \lambda_g(e_G) = ge_G = g$, so $g = e_G$. □(Claim)

By the first isomorphism theorem, $G/\operatorname{Ker}(\varphi) \cong \operatorname{Im}(\varphi)$. Denote by H the image of φ. $H \leq S_G$.
$G/\operatorname{Ker}(\varphi) = G/\{e_G\} \cong G$, so $G \cong H$. □(Theorem)

Example. A concrete example:
$G = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) = \{1, a, b, c\}$

$$\lambda_b : \begin{cases} 1 \mapsto 3 \\ 2 \mapsto 4 \\ 3 \mapsto 1 \\ 4 \mapsto 2 \end{cases} \quad \text{Run cycle decomposition on each}$$

$G \cong \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4), (2\ 3)\} \leq S_4$.
This is sometimes called the left multiplication permutation representation of a group.

Remark. Cayley's theorem is not always "optimal." Sometimes $|G| = n$ and $m < n$ such that $H \leq S_m$ and $G \cong H$.

Example. $(\mathbb{Z}/6\mathbb{Z}) = G, |G| = 6$. Take $\sigma = (1\ 2\ 3)(4\ 5) \in S_5$.
Then $H = \langle\sigma\rangle \cong (\mathbb{Z}/6\mathbb{Z}) = G$, but $H \leq S_5$ and $5 < 6$.

Orbit Equivalence Relations

Definition 63. Suppose $G \curvearrowright X$. Define a relation $\sim$ on X by $x \sim y$ iff $\exists g \in G : g \cdot x = y$. This $\sim$ is called the orbit equivalence relation.

Proposition 64. *$\sim$ is an equivalence relation.*

Proof. 3 properties:

- Reflexivity:
  $x \in X$. $e_G \cdot x = x$, so $x \sim x$
- Symmetry:
  Suppose $x \sim y$. Fix $g \in G$ such that $g \cdot x = y$. Compute $g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = (gg^{-1}) \cdot x = e_G \cdot x = x$. So $y \sim x$
- Transitivity:
  Suppose $x \sim y, y \sim z$. Fix $g, h \in G$ such that $g \cdot x = y$ and $h \cdot y = z$. So $(hg) \cdot x = h \cdot (g \cdot x) = h \cdot y = z$, so $x \sim z$

It follows that $\sim$ is an equivalence relation. □

Definition 65. The equivalence classes of $\sim$ are called orbits. Write them like $\mathcal{O}_x$. Because $\sim$ is an equivalence class, $\{\mathcal{O}_x\}_{x \in X}$ partitions X.

Notation. Sometimes we write $G \cdot x$ to denote the orbit of x.

Lecture 13 (2016–02–12).

Definition 66. $G \curvearrowright X$, fix $x \in X$. The stabilizer of x is $G_x = \{g \in G : g \cdot x = x\} \subseteq G$.

Proposition 67. *If G is a group then $G_x \leq G$.*

Proof. Homework Question □

Example. Let's look at some examples of group actions and stabilizers of some the elements of the sets they act on.

(1) $\sigma \in S_5$, say $\sigma = (1\ 3\ 4)(2\ 5)$. $S_5 \curvearrowright \{1, 2, 3, 4, 5\}$. This induces an action of $\langle \sigma \rangle \curvearrowright \{1, 2, 3, 4, 5\}$. (Note that $|\sigma| = 6$.)
   $G = \langle \sigma \rangle = \{e, \sigma, \ldots, \sigma^5\}$. $X = \{1, 2, 3, 4, 5\}$. Look at $x = 3$. $\mathcal{O} = \{1, 34\}$ = the cycle containing 3 in the cycle decomposition of σ.
   If we check each exhaustively, we find $e \cdot 3 = 3$ and $\sigma^3 = 3$ so the stabilizer of G_3 is $\{e, \sigma^3\}$.
   In general, if you have any perm group, the orbit of an element of the cyclic subgroup generated by an element in the permutation group is going to be the cycles and the stabilizers are going to be the lengths of the cycles.

(2) $G \curvearrowright G$ by left multiplication. $g \cdot x = gx$
   Claim. $\forall x \in G$, $\mathcal{O}_x = G$ (its orbit is G).

Proof. Fix $x \in G$, Fix $g \in G$. Choose $h = gx^{-1}$, then $h \cdot x = (gx^{-1}) \cdot x = (gx^{-1})x = g(x^{-1}x) = g$. Thus, $g \in \mathcal{O}_x$. Thus, $\mathcal{O}_x = G$. □

Claim. $\forall x \in G, G_x = \{e_G\}$.

Proof. Fix x. Suppose $g \in G$. $g \cdot x = x$.
Thus, $gxx^{-1} = xx^{-1}$ (as $X = G$), so $g = e_G$. □

(3) $S_3 \curvearrowright S_3$ by conjugation. $g \cdot x = gxg^{-1}$.
Orbits $\{e\}, \{(1\ 2), (1\ 3), (2\ 3)\}, \{(1\ 2\ 3), (1\ 3\ 2)\}$
The stabilizer of $(1\ 2)$ is $\{e, (1\ 2)\}$.

(4) $H \leq G$. Let $H \curvearrowright G$ by right multiplication. Then

$$\mathcal{O}_{x \in G} = \{h \cdot x : h \in H\} = \{xh^{-1} : h \in H\} = \{xh : h \in H\} = xH.$$

Thus, the orbits of the elements of G are the left cosets of H in G.

Definition 68. Suppose $G \curvearrowright X$ with a single orbit $\mathcal{O} = X$.
We say that the action is transitive

Definition 69. Orbits of the conjugation action of $G \curvearrowright G$ are called conjugacy classes.

Theorem 70 (Orbit-Stabilizer Theorem)**.** *Suppose G is a finite group, X is some set, and $G \curvearrowright X$. Fix arbitrarily $x \in X$ with orbit $\mathcal{O} \subseteq X$ and stabilizer $G_x \leq G$. Then $|\mathcal{O}| \cdot |G_x| = |G|$.*

Proof. Define two equivalence relations on G.

(1) $g \sim h$ iff $g^{-1}h \in G_x$ (left coset equivalence of stabilizers)
(2) $g \approx g$ iff $g \cdot x = h \cdot x \in X$

For the reader: check $\sim$ and $\approx$ are equivalence relations.

Claim (1). Each $\sim$ equivalence class has $|G_x|$ many elements in it.

Proof. Already done □(Claim 1)

Claim (2). There are exactly $|\mathcal{O}|$-many $\approx$ equivalence classes.

Proof. For each $y \in \mathcal{O}$, put $A_y = \{g \in G : g \cdot x = y\}$. The collection of $\{A_y : y \in \mathcal{O}\}$ is exactly the set of $\approx$-equivalent classes.
In other words, $\approx$ is partitioning G by the elements which move x into each particular element of $\mathcal{O}$. □(Claim 2)

Claim (3). $\sim \cong \approx$

Proof. First show $g \sim h \implies g \approx h$, then show $g \approx h \implies g \sim h$.

- Suppose $g^{-1}h \in G_x$, then $(g^{-1}h) \cdot x = x$, so $g^{-1} \cdot (h \cdot x) = x$.
  Act by g on both sides. $g \cdot x = g \cdot (g^{-1} \cdot (h \cdot x)) = (gg^{-1}) \cdot (h \cdot x) = h \cdot x$, so $g \approx h$.
- Suppose $g \cdot h = h \cdot x$. Act by g^{-1} on both sides. $g^{-1} \cdot (g \cdot h) = g^{-1}(h \cdot x)$.
  $x = e_G \cdot x = (g^{-1}h) \cdot x$, thus $g^{-1}h \in G_x$.

□(Claim 3)

So the upshot is that we have a single equivalence relation on G. It has $|\mathcal{O}|$ -many classes. Each class has $|G_x|$-many elements. Hence $|G| = |\mathcal{O}| \cdot |G_x|$. □(Theorem 70)

Remark. The above theorem also works when G is not finite, however it involves multiplication of ordinals, which is beyond the scope of this course.

Lecture 14 (2016–02–15). We will continue referencing the Orbit-Stabilizer Theorem for the rest of the week

Example. Fix $p \geq 2$ prime and $c \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$. How many distinct (up to rotation) necklaces can you make of length p out of c colors of beads?
More formally, let $X = \{\text{sequences of length } p \text{ with entries in } \{1, 2, \ldots, c\}\}$. Also, let $G = (\mathbb{Z}/p\mathbb{Z})$ act on X by "rotating the indices" $\pmod p$.
For example, if $x = (1, 2, 1, 2, 3) \in X$, then $\overline{1} \cdot x = (3, 1, 2, 1, 2), \overline{3} \cdot x = (1, 2, 3, 1, 2)$.
Question: How many orbits does this action have?
We know by the Orbit-Stabilizer Theorem that for any $x \in X$, $|\mathcal{O}_x| \cdot |G_x| = |G| = p$. Thus $\{|\mathcal{O}_x|, |G_x|\} = 1, p$. Thus, let us pick an arbitrary necklace $x \in X$ and examine $\mathcal{O}_x$ and G_x.

Case 1: $|\mathcal{O}_x| = 1$. Then $|G_x| = p$. So $g \cdot x = x$ for *all* $g \in (\mathbb{Z}/p\mathbb{Z})$. This necessitates that every bead in x is the same as the next one, meaning all the beads on x are the same color. As there are c colors, there are exactly c-many possible distinct $x \in X$ in this case.

Case 2: $|\mathcal{O}_x| = p$. Then $|G_x| = 1$. All other $x \in X$ fall into this case. $|X| = c^p$ as there are p places with c choices each. Thus there are $c^p - c$ necklaces falling into this case.

Thus, the total number of orbits is $c + \frac{c^p - c}{p}$. As a nice corollary, this implies that $\frac{c^p - c}{p}$ is an integer, as it is counting something.

Next, we make necklaces out of group elements.

Theorem 71 (Cauchy)**.** *Suppose that G is a finite group $|G| = n$ and $p \geq 2$ is a prime such that $p|n$. Then $\exists g \in G$ such that $|g| = p$.*

Proof. Let X be the set of sequences $(g_1, g_2, \ldots, g_p)$ of length p with elements from G, such that $\prod_{i=1}^{p} g_i = e_G$.
Claim (1). $|X| = n^{p-1}$

Proof. Fix $g_1, \ldots, g_{p-1}$. Then $g_p = (g_1 g_2 \ldots g_{p-1})^{-1}$ is the unique way to land in X. $\square$(C1)

Claim (2). Suppose $(g_1, g_2, \ldots, g_p) \in X$. Then $(g_p, g_1, g_2, \ldots g_{p-1}) \in X$.

Proof. We know $\prod_{i=1}^{p} g_i = e_G$. Multiplying both sides on the right by g_p^{-1} gives $\prod_{i=1}^{p-1} g_i = {g_p}^{-1}$. Then, we multiply on the left by g_p. to get $g_p \prod_{i=1}^{p-1} g_i = e_G$. Note that this is simply conjugating by g_p. $\square$(C2)

Let $H = (\mathbb{Z}/p\mathbb{Z})$, $H \curvearrowright X$ by "rotation." So, $\overline{1} \cdot (g_1, g_2, \ldots, g_p) = (g_p, g_1, \ldots, g_{p-1})$. By claim 2, we note that this is a group action. By the Orbit-Stabilizer Theorem , we have for every $x \in X, |\mathcal{O}_x| \cdot |H_x| = |H| = |(\mathbb{Z}/p\mathbb{Z})| = p$. So for every $x \in X, \mathcal{O}_x = 1$ or p.
Let's say k_1 is the number of orbits of cardinality 1, and k_p is the number of orbits of cardinality p.
Hence, $1 \cdot k_1 + p \cdot k_p = |X| = n^{p-1}$, so $k - 1 = n^{p-1} - p \cdot k_p$. Thus $p|k$.
Claim (3). $k_1 \geq 1$.

Proof. $(\underbrace{e_G, e_G, \ldots, e_G}_{p \text{ times}}) \in X$ $\square$(C3)

Thus, by claim 3 and the fact that $p|k$, $k_1 \geq p$. In particular, $k_1 \geq 2$. So there is some $x \in X$ with $x \neq (e_G, e_G, \ldots, e_G)$ such that $\mathcal{O}_x = 1$. So $x = (\underbrace{g, g, \ldots, g}_{p \text{ times}})$ with $g \neq e_G$.

$x \in X \implies \prod_{i=1}^{p} g = e_G \implies g^p = e_G$. Thus $|g| = p$, so we're done. $\square$(Cauchy)

Remark. The above theorem is *false* if p were to be composite.

Lead in to next lecture: Conjugation.
Let $G \curvearrowright G$ by conjugation. $\forall g \in G, \forall x \in G : g \cdot x = gxg^{-1}$
If $x \in G$, what is G_x (under conjugation)?

$$G_x = \{g \in G : g \cdot x = x\} = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\}$$

In other words, $G_x = \{g \in G : g \text{ commutes with } x\}$.

Definition 72. The center of G, denoted $Z(G)$ is the set $\{x \in G : \forall g \in G(gx = xg)\}$.

So $x \in Z(G) \iff G_x = G$ (for conjugation). This is also equivalent to saying $\mathcal{O}_x = \{x\}$.

Lecture 15 (2016–02–17).

Class Note

Midterm coming up: February 26th in class (1:30-2:20pm)
Class Plans: Up to spring break, we'll continue talking about groups
After spring break, we'll start ring theory.

Definition 73. $G \curvearrowright X$ $x \in X$ is a fixed point of the action if $\forall g \in G(g \cdot x) = x$. (This is equivalent to saying $G_x = G$, or $\mathcal{O}_x = \{x\}$.)

Example.

(A) $(\mathbb{Z}/n\mathbb{Z})$ acts by "rotation" on "c^n" = sequences of length n with elements in $\{1, 2, \ldots, c\}$. Then the fixed points are the constant sequences.
(B) $G \curvearrowright G$ by left or right multiplication and $G \neq \{e_G\}$, then there are *no* fixed points. (Take $g \neq e_G$, then $g \cdot h = gh \neq h$.)
(C) $G \curvearrowright G$ by conjugation. $g \cdot x = gxg^{-1}$. Then x is a fixed point iff $x \in Z(G)$, i.e., $\forall g \in G(xg = gx)$, x commutes with everything in G.

Definition 74. Given a prime $p \geq 2$, we say that a finite group G is a p-group if $|G| = p^k$ for some $k \in \mathbb{N}^+$.

Proposition 75. *The following are equivalent:*

(1) G is a p-group
(2) Every subgroup $H \leq G$ is a p-group
(3) Every $g \in G$ has $|g| = p^i$ for some $i \in \mathbb{N}$

Proof. Left to the reader. $\square$

Theorem 76 (Fixed-Point Lemma)**.** *Suppose p prime, G is a p-group and $G \curvearrowright X$, and let F be the number of fixed points. Then, $F \equiv |X| \pmod{p}$.*

Proof. Say $|G| = p^k$. By the Orbit-Stabilizer Theorem, for $x \in X$, $|\mathcal{O}_x| \cdot |G_x| = p^k$. so $|\mathcal{O}_x| \in \{1, p, p^2, \ldots, p^k\}$.

For $0 \leq i \leq k$, denote by n_{p_i} the number of orbits of size p^i.

$$|X| = \sum_{i=0}^{k} p^i \cdot n_{p^i}$$

as the orbits partition X. Thus, $|X| - n_1 = \sum_{i=1}^{k} p^i \cdot n_{p^i}$, so $p|(|X| - n_1)$. It follows that $n_1 \equiv |X| \pmod{p}$, as desired. □(Lem)

Corollary 77. *Suppose p prime and $G \neq \{e\}$ is a p-group. Then $|Z(G)| \geq p$.*

Proof. $|Z(G)|$ = number of fixed points of $G \curvearrowright G$ by conjugation. Thus, by the Fixed-Point Lemma, $|Z(G)| \cong |G| \pmod{p}$. So, $|Z(G)|$ is a multiple of p.

Claim. $|Z(G)| \neq 0$. This is true as $e_G \in Z(G)$.

Thus, $|Z(G)| \geq p$. □(Cor)

Proposition 78. *Suppose p prime, G is a group with $|G| = p^2$. Then, $G \cong (\mathbb{Z}/p^2\mathbb{Z})$ OR $G \cong ((\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z}))$.*

Proof. If $\exists g \in G$ with $|g| = p^2$ then $\langle g \rangle = G$, so $G \cong (\mathbb{Z}/p^2\mathbb{Z})$.
Otherwise, all non-identity elements of G have order p.
Since $|Z(G)| \geq p \geq 2$, we may fix non-identity $h \in Z(G)$ The set $\langle h \rangle$ has cardinality p. Now pick $k \in G \setminus \langle h \rangle$. Put $H := \langle h \rangle$ and $K := \langle k \rangle$, both with cardinality p.

Claim. The map $\varphi : ((\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})) \to G$ with $\varphi(\overline{i}, \overline{m}) = h^i k^m$ is an isomorphism. ($\overline{i}$ and $\overline{m}$ are residue classes of $(\mathbb{Z}/p\mathbb{Z})$.) Note that if $i, j \in \overline{i}$, then $h^i = h^j$, so $h^i (h^j)^{-1} = h^{i-j} = h^{pa} = e_G$.

Proof. First we show φ is a homomorphism, i.e., $\varphi(\overline{i}+\overline{j}, \overline{m}+\overline{n}) = (h^i k^m)(h^j k^n) = \varphi(\overline{i}, \overline{m})\varphi(\overline{j}, \overline{n})$.
It is apparent that $\varphi(\overline{i} + \overline{j}, \overline{m} + \overline{n}) = h^{i+j} k^{m+n} = h^i h^j k^m k^n$. However, as h is in the center of G, h and k commute, so $h^i h^j k^m k^n = h^i k^m h^j k^n$ as desired.
Next we show that φ is an isomorphism by showing it is also a bijection.
Since $|((\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z}))| = |G| = |p^2|$, to show φ is bijective, it suffices to show that φ is *injective*. In turn, it is sufficient to prove $\mathrm{Ker}(\varphi) = \{e_G\}$.
As we proved in a homework, $H \cap K \leq H$, so $|H \cap K|$ is 1 or p. $k \notin H \cap K$, so $|H \cap K| \lneq |K|$. Thus, as the cardinality of the intersection must divide p^k, the intersection has cardinality 1, meaning $H \cap K = \{e_G\}$
Suppose $\overline{i}, \overline{m} \in (\mathbb{Z}/p\mathbb{Z})$ with $\varphi(\overline{i}, \overline{m}) = e_G$. Then $h^i k^m = e_G$. Thus, $\underbrace{h^i}_{\in H} = \underbrace{k^{-m}}_{\in K}$. Since $h^i = k^{-m} \in H \cap K$, $h^i = k^{-m} = e_G$. So i, m are multiples of p. Hence, $(\overline{i}, \overline{m}) = (\overline{0}, \overline{0})$. Thus $\mathrm{Ker}(\varphi) = \{e_G\}$, so φ is injective as desired, meaning φ is an isomorphism. □(prop)

□

Lecture 16 (2016–02–19).

Class Note
Review sheet for Midterm 1 will be posted this afternoon. (Exam on February 26th in class).

Conjugation in S_n.

Example. Suppose $\sigma = (1\ 3\ 4)(2\ 5) \in S_5$ and $\tau = (1\ 2\ 3\ 4\ 5) \in S_5$. What is $\tau\sigma\tau^{-1}$?
Compute $\tau^{-1} = (1\ 5\ 4\ 3\ 2)$.
So, $\tau\sigma\tau^{-1} = (1\ 2\ 3\ 4\ 5)(1\ 3\ 4)(2\ 5)(1\ 5\ 4\ 3\ 2) = (1\ 3)(2\ 4\ 5)$

Proposition 79. *Suppose $\sigma, \tau \in S_n$. Fix $a, b \in \{1, 2, \ldots, n\}$. Suppose $\sigma' := \tau\sigma\tau^{-1}$. If $\sigma(a) = b$ then $\sigma'(\tau(a)) = \tau(b)$*

Proof. $\sigma'(\tau(a)) = (\tau\sigma\tau^{-1}\tau)(a) = (\tau\sigma)(a) = \tau(b)$. □

But why is this useful? Conjugation in S_n is "relabeling." Revisiting the previous example:
$\sigma = (1\ 3\ 4)(2\ 5)$ $\tau\sigma\tau^{-1} = (\tau(1)\ \tau(3)\ \tau(4))(\tau(3)\ \tau(5)) = (2\ 4\ 5)(3\ 1) = (1\ 3)(2\ 4\ 5)$.
We've shown: Whenever σ, σ' are conjugate in S_n, then σ, σ' have the same cycle type (i.e. the same number of cycles of each length).

Definition 80. The cycle type of a permutation is the number of cycles of each length in the permutation's cycle decomposition

Theorem 81. *$\sigma, \sigma' \in S_n$ are conjugate (in S_n) if and only if they have the same cycle type.*

Sketch. We know that conjugate $\implies$ same cycle type. For the converse, suppose σ, σ' have the same cycle type.
Shuffle the cycles (because they're disjoint) in σ to line up with those of σ.
Then take the permutation that takes the elements in the cycles of σ to the corresponding elements in the cycles of σ'. (Also, make sure that fixed points are sent to fixed points.)
This generates a permutation τ such that $\tau\sigma\tau^{-1} = \sigma'$, so σ and σ' are conjugate. □(sketch)

Example. $\sigma = (1\ 3)(2\ 5\ 6)(4\ 7) \in S_7$ $\sigma' = (1\ 5\ 7)(2\ 3)(4\ 6) \in S_7$.
Thus, by our last theorem, they are conjugate.
Shuffle σ' to corespond with σ:
$\sigma = (1\ 3)(2\ 5\ 6)(4\ 7)$
$\sigma' = (2\ 3)(1\ 5\ 7)(4\ 6)$
Thus, $\tau = (1\ 2)\cancel{(3)}\cancel{(4)}\cancel{(5)}(6\ 7)$.
Note that we could have shuffled the cycles differently and come up with a different τ.

Example. Compute the size of every conjugacy class in S_4. (Where the conjugacy classes are the orbits of $S_4 \curvearrowright S_4$ by conjugation).
By our previous theorem we only have to check each cycle type.

Cycle Types:	How many with that type?
$(\cdot\ \cdot\ \cdot\ \cdot)$	$3! = 6$
$(\cdot\ \cdot\ \cdot)$	$\binom{4}{3} \cdot 2! = 8$
$(\cdot\ \cdot)\ (\cdot\ \cdot)$	$\binom{4}{2} \cdot \binom{2}{2} \cdot \frac{1}{2!} \cdot 1! \cdot 1! = 3$
$(\cdot\ \cdot)$	$\binom{4}{2} \cdot 1! = 6$
e	1
Total:	24

Example. How many elements of S_5 commute with $\sigma = (1\ 4)(3\ 5)$? Use the Orbit-Stabilizer Theorem!
$S_5 \curvearrowright S_5$ by conjugation. $\mathcal{O}_\sigma =$ the conjugacy class of σ.
$G_\sigma = \{g \in S_5 : g\sigma g^{-1} = \sigma\} = \{g \in S_5 : g\sigma = \sigma g\}$. The Orbit-Stabilizer Theorem says taht $|\mathcal{O}_\sigma| \cdot |G_\sigma| = |S_5|$ Thus, as $|\mathcal{O}_\sigma| = 15$ and $|S_5| = 120$ so $|G_\sigma| = \frac{120}{15} = 8$.

Example. How many elements of S_9 commute with $\sigma = (1\ 2)(3\ 4)(5\ 6)(7\ 8\ 9)$?

The size of σ's conugacy class is $n = \binom{9}{2}\binom{7}{2}\binom{5}{2}\frac{1}{3!}1!1!1!2!$
Thus, the number of elements of S_9 commuting with σ is $\frac{9!}{n} =$

Lecture 17 (2016–02–22).

Definition 82. If $A, B \subseteq G$, where G is a group (A and B not necessarily). Then put $AB := \{ab : a \in A, b \in B\}$. We note that unless the group is abelian, order still matters.
Caveat: If $H, K \leq G$ are subgroups, then HK is typically *not* a subgroup.

Proposition 83. *If G is a finite group and $H, H \leq G$ are subgroups, then $|HK| = \frac{|H|\cdot|K|}{|H\cap K|}$.*

Proof. Note that $HK = \{hk : h \in H, k \in K\} = \bigcup_{h\in H} hK$. So $|HK| = n \cdot |K|$, where n is the number of left cosets of K meeting H.

Claim. For $h_1, h_2 \in H$: $h_1K = h_2K \iff h_1^{-1}h_2 \in H \cap K$

Proof. ($\implies$): If $h_1K = h_2K$, then by definition of coset equality, we know that $h_1^{-1}h_2 \in K$. As H is a subgroup of G, $h_1^{-1}h_2 \in H$ also.
($\impliedby$): If $h_1^{-1}h_2 \in H \cap K$, it's in K, so $h_1K = h_2K$. □(Claim)

Note that $H \cap K \leq H$. So the number of cosets of $H \cap K$ in H is $\frac{|H|}{|H\cap K|}$. Thus, $n = \frac{|H|}{|H\cap K|}$, meaning that $|HK| = \frac{|H|\cdot|K|}{|H\cap K|}$, as desired. □

Remark. The proposition is especially useful when $H \cap K = \{e_G\}$. In this case, you get $|HK| = |H| \cdot |K|$. This happens, for example, when

- $|H|, |K|$ are relatively prime
- $|H| = |K| = p$ prime, and $H \neq K$.

Corollary 84. *Suppose G is a finite group, and $H, K \leq G$ such that*

(1) $|G| = |H| \cdot |K|$
(2) $H \cap K = \{1\}$.
(3) $\forall h \in K, \forall k \in K : hk = kh$.

Then $G \cong H \times K$.

Proof. Consider the map $\varphi : H \times K \to G$ with $\varphi((h, k)) = hk$.

Claim (1). φ is a homomorphism.

1. Suppose $(h_1, k_1), (h_2, k_2) \in H \times K$. First compute $\varphi((h_1, k_1)(h_2, k_2)) = \varphi((h_1h_2, k_1k_2)) = h_1h_2k_1k_2$. Then compute

$$\begin{aligned}&\varphi((h_1, k_1))\varphi((h_2, k_2))\\ &= (h_1k_1, h_2k_2)\\ &= h_1(k_1h_2)k_2\end{aligned}$$

As $hk = kh$ by assumption

$$\begin{aligned}&= h_1h_2k_1k_2\\ &= \varphi((h_1, k_1)(h_2, k_2))\end{aligned}$$

So φ is a homomorphism. □(C1)

Claim (2). φ is a bijection.

2. Note $|G| = |H| \cdot |K| = |H \times K|$, which are both finite. So, it suffices to show that φ is a surjection.
$\varphi[H \times K] = \{hk : h \in H, k \in K\} = HK$, and $|HK| = \frac{|H| \cdot |K|}{H \cap K}$. Thus $\mathrm{Im}(\varphi) = G$, so φ is surjective. □(C2)

It follows that φ is an isomorphism, so $G \cong H \times K$ as desired. □(Cor)

Theorem 85. *Suppose G is finite and $H, K \trianglelefteq G$, such that:*

- $|G| = |H| \cdot |K|$
- $H \cap K = \{e_G\}$

Then $G \cong H \times K$.

Proof. By corollary 84, it suffices to show that $\forall h \in H, \forall k \in K : hk = kh$. Consider $hkh^{-1}k^{-1}$ (called the commutator).

Claim (1). $hkh^{-1}k^{-1} \in H$

Which is proved by inserting parentheses as follows:

$$\underbrace{h}_{\in H}\underbrace{(kh^{-1}k^{-1})}_{\in H} \in H,$$

where the second containment holds because H is normal.

Claim (2). $hkh^{-1}k^{-1} \in K$. This is true because$(hkh^{-1})k^{-1} \in K$, as K is normal.

Thus, $hkh^{-1}k^{-1} \in H \cap K = \{e_G\}$. So, $hkh^{-1}k^{-1} = e_g \implies hk = kh$. □(Thm)

Next, we act on the set of subgroups by conjugation.

Proposition 86. *Let G be a group $H \leq G$ a subgroup, $g \in G$. Then $gHg^{-1} = \{ghg^{-1} : h \in H\}$ is a subgroup of G. Moreover, $gHg^{-1} \cong H$.*

Proof. Put $H' = gHg^{-1}$.
H' is nonempty as $ge_Gg^{-1} = e_G \in H'$.
H' is closed under products because if $gh_1g^{-1}, gh_2g^{-1} \in H'$, then $(gh_1hg^{-1})(gh_2g^{-1}) = g(h_1h_2)g^{-1} \in H'$.
H' is closed under inverses as if $ghg^{-1} \in H$, then $(ghg^{-1})^{-1} = (g^{-1})^{-1}h^{-1}g^{-1} = ghg^{-1} \in H'$

Claim. $\varphi : H \to H'$, $\varphi(h) = ghg^{-1}$ is an isomorphism.

The proof is left as an exercise to the reader. □

Hence, G acts on $\{H : H \leq G\}$ by conjugation $g \cdot H = gHg^{-1}$.
In addition, H is a fixed point of this action exactly when $H \trianglelefteq G$.

Lecture 18 (2016–02–24).

Theorem 87. *Suppose $p < q$ primes and $q \not\equiv 1 \pmod{p}$. Then every group G with $|G| = pq$ is cyclic. (i.e., $G \cong (\mathbb{Z}/pq\mathbb{Z})$)*

Proof. Let $p = 3, q = 5$, The general case proof is left as an exercise.
Note: $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$ is cyclic because $|(h, k)| = \mathrm{lcm}(p, q) = pq$ (as they're relatively prime).
So now there is enough to show that $G \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$. By Cauchy, we may take subgroups $H, K \leq G$ with $|H| = p$ and $|K| = q$. We want: $\forall h \in H, \forall k \in K : hk = kh$ (then $G \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$).

First we let K act on the subgroups of G by conjugation. $k \cdot J = kJk^{-1}$
$|K| = 5$, so every orbit has size 1 or 5 by the Orbit-Stabilizer Theorem. In particular, the orbit of H $\mathcal{O}_H$ has size 1 or 5.

Case 1. $|\mathcal{O}_H| = 1$. I.e., $\forall k \in K : kHk^{-1} = \{khk^{-1} : h \in H\} = H$.
Now let $K \curvearrowright H$ by conjugation. $k \cdot h = khk^{-1}$. Orbits have size 1 or 5. But $|H| = 3$ So every orbit has size 1. I.e., $\forall k \in K, \forall h \in H : khk^{-1} = h$, so $kh = hk$. Hence (in this case), $G \cong H \times K$.

Case 2. $|\mathcal{O}_H| = 5$ I.e., there are 5 distinct subgroups of the form $kHk^{-1}, k \in K$. Then $G = \bigcup_{S \in \mathcal{O}_H} S \cup K$, as each pair of subgroups in $\mathcal{O}_H$ has intersection e_G. Also K exists, so the subgroups of G are either in $\mathcal{O}_H$ or equal to K. Thus, K is the *unique* subgroup of G of cardinality 5. In particular, $\forall g \in G : gKg^{-1}$ also has cardinality 5, so $gkg^{-1} = K$, hence $K \trianglelefteq G$. Let $H \curvearrowright K$ by conjugation. $h \cdot k = hkh^{-1} \in K$.

Claim (1). $\exists k_0 \in K$ such that $k_0 \neq e_G$ and $\forall h \in H : hk_0h^{-1} = k_0$

Proof. Let p be the number of fixed points. By Fixed-Point Lemma,$p \equiv |K| \pmod 3$. However, $|K| \not\equiv 1 \pmod 3$, so $p \geq 2$. Thus, there exists a non-identity fixed point (k_0)[1]. □(Claim)

So, $\forall h \in H : hk_0 = k_0h$. Since $k_0 \neq e$, $|k_0| = 5$, hence $K = \langle k_0 \rangle$. Since $hk_0^n = k_0^n h$, and h was arbitrary, we know that $\forall h \in K, \forall k \in K : hk = kh$. Thus, $G \cong H \times K$. □(Thm).

Proposition 88. *(p=2) Suppose $q > 2$ is prime. Then there exists (up to isomorphism) a* unique *non-cyclic group G with $|G| = 2q$.*

Proof Sketch. Fix (by Cauchy) $x, y \in G$ such that $|x| = 2$, $|y| = q$, then put $H = \langle x \rangle$ and $K = \langle y \rangle$.
We posit that $K \trianglelefteq G$ (verification left as an exercise).
So $H \curvearrowright K$ by conjugation. So, $xyx^{-1} \in K$ $\exists r : 0 < r < q$ such that $xyx^{-1} = y^r$, $xy^2x^{-1} = (xyx^{-1})(xyx^{-1}) = y^{2r}$. Thus, it is apparent that $xy^jx^{-1} = y^{jr \pmod q}$
But also,

$$y = x^2y^2x^{-2} = x(xyx^{-1})x^{-1} = x(y^r)x^{-1} = y^{r \cdot r}$$

So, $r^2 \equiv 1 \pmod q$
Exercise: The only solutions to $r^2 \equiv q \pmod{()q}$ are $r \equiv 1, -1 \pmod q$.

Case 1. $(r = 1)$: $xyx^{-1} = y$, i.e., $xy = yx$. Hence, $G \cong \langle x \rangle \times \langle y \rangle = H \times K$, cyclic.

Case 2. $(r = -1)$: $xyx^{-1} = y^{-1}$. Shuffle to obtain $yx = xy^{-1}$.

We know that $G = \{x^iy^j : i \in \{0, 1\}, j \in \{0, \ldots, q-1\}\} = HK$.

To multiply, $(x^iy^j)(x^\ell y^k) = \begin{cases} (x^iy^{j+k}) & \text{if } \ell = 0 \\ x^i(y^jx)y^k = x^ixy^{-j}y^k = x^{i+1}y^{k-j} & \text{if } \ell = 1 \end{cases}$

Hence, the group operation is completely determined by $yx = xy^{-1}$, and so there is at most one non-cyclic group (up to isomorphism) of cardinality $(\mathbb{Z}/q\mathbb{Z})$.
To show the existance of such a group, given $n \geq 3$, we consider the dihedral group of cardinality $2n$, where the dihedral group is the group generated by reflection and rotation on the regular n-polygon. □

Lecture 19 (2016–02–29).

[1]Note that this is where we needed the hypothesis that $q \not\equiv 1 \pmod p$.

Definition 89. Let $H \leq G$ be groups. The normalizer of H in G is $N_G(H) = N(H) = \{g \in G : g^{-1}Hg = H\} = \{g \in G : gHg^{-1} = H\}$

Fact/Exercise:

(1) $N(H) \leq G$
(2) $H \trianglelefteq N(H)$

Theorem 90 (Sylow 1)**.** *Suppose that G is a finite group, p is prime, and p^i divides $|G|$ for some $i \in \mathbb{Z}$. Then $\exists H \leq G$ such that $|H| = p^i$.*

Proof. Proceed by induction on i.
If $i = 0$ then trivial as $H = \{e\}$, the trivial subgroup. If $i = 1$ then this is true by Cauchy.
Our stategy is to suppose we have $H_i \leq G$ of cardinality $|H_i| = p^i$. and p^{i+1} divides $|G|$. We will find $H_{i+1} \supseteq H_i$ with $H_{i+1} \leq G$ and $|H_{i+1}| = p^{i+1}$.
Intuition: Consider the cosets of H_i in G. We're going to pick out p cosets of H_i $g_1Hg_2H, \ldots, g_pH$ such that $\bigcup_{i=1}^{p} g_iH$ is a subgroup of G.
Let $X = G/H_i = \{gH_i : g \in G\}$. Note that $|X| = \frac{|G|}{|H_i|} = \frac{p^z m}{p^i}$(where $z > i$) $\equiv 0 \pmod p$.
Let $H_i \curvearrowright X$ by left multiplication. $h \cdot (gH_i) = (hg)H_i$.

Claim (1). $gH_i \in X$ is a fixed point of the action iff $g \in N(H_i)$.

Proof. gH_i is a fixed point iff $\forall h \in H_i(h \cdot (gH_i) = gH_i)$ iff $(hg)H_i = gH_i$ iff $g^{-1}hg \in H_i$.
Thus, $g^{-1}H_ig \in H_i$ so, as they are finite sets with the same cardinality and conjugation is an injective map, $g^{-1}H_ig = H_i$, meaning $g \in N(H_i)$ $\square$(C1)

By Fixed-Point Lemma, since H_i is a p-group, we know that # fixed points $\equiv |X| \pmod p$. The number of cosets fixed by the action is a multiple of p. This is equivalent to saying p divides $|N(H_i)/H_i|$ (i.e., the number of cosets represented in the normalizer is a multiple of p). Since $H_i \trianglelefteq N(H_)i$, $N(H_i)/H_i$ is a quotient group. So by Cauchy, we may take $g \in N(H_i)$ such that $|gH_i| = p$ in $N(H_i)/H_i$.
Intuition: As we cycle through the powers of g, we get the cosets we're going to choose.
Finally, let $H_{i+1} = \bigcup_{k=0}^{p-1} g^kH_i = \{g^kh : h \in H, 0 \leq k < p\}$.
Note that $|H_{i+1}| = p^{i+1}$ as it's a union of p disjoint cosets of cardinality p^k.

Claim (2). H_{i+1} is a subgroup of G.

Proof.

- $e_G \in H_{i+1}$
- $h_1, h_2 \in H_{i+1} \implies h_1h_2 \in H_{i+1}$
  Fix k, ℓ such that $x, y \in H_i$ and $h_1 = g^kx, h_2 = g^\ell y$.
  Since $g \in N(H_i), \exists z \in H_i$ such that $g^{-\ell}xg^\ell = z$. So,
  $$h_1h_2 = g^kxg^\ell y = g^{k+\ell} \underbrace{zy}_{\in H_i} \in H_{i+1}$$

$\square$(C2)

$\square$(Thm)

Definition 91. For p prime, $H \leq G$ (finite),is a Sylow p-subgroup if $|H|$ is the largest power of p dividing $|G|$. i.e., if, $|G| = p^km, \gcd(p, m) = 1$. Then $|H| = p^k$.

Theorem 92 (Sylow 2)**.** *Any two Sylow p-subgroups of G (finite) are conjugate.*

Proof will come later.

Theorem 93 (Sylow 3)**.** *If $|G| = p^k m, \gcd(p, m) = 1$, then the number of Sylow p-subgroups n_p satisfies $n_p | m$ and $n_p \equiv 1 \pmod{p}$.*

Proof will come next lecture, first let's see an example.

Example.

a) Every group G with $|G| = 15 = 3 \cdot 5$ is cyclic.
   $n_3 | 5 \implies n_3 \in \{1, 5\}$ and $n_3 \equiv 1 \pmod 3$, so $n_3 = 1$. $n_5 = 1$. Thus, $\exists H, K \trianglelefteq G$ with $|H| = 3, |K| = 5$. So, by Corollary 84, $G \cong H \times K$.
b) There are (up to isomorphism) exactly two groups G with cardinality $99 = 3^2 \cdot 11$. Sylow 3-subgroup has cardinality 9. $n_3 = \#$ of subgroups of cardinality 9.
   $n_3 | 11 \implies n_3 \in \{1, 11\}$. As $n_3 \equiv 1 \pmod 3$, it can't be 11, so $n_3 = 1$
   $n_{11} = \#$ of subgroups of cardinality 11. $n_{11} | 9$ and $n_{11} \cong 1 \pmod 1 1$ means that $n_{11} = 1$.
   Fix unique $H, k \trianglelefteq G$ with $|H| = 9, |K| = 11, H \cap K = \{e\}$. So $G \cong H \times K$.
   Case 1: $H \cong \mathbb{Z}/9\mathbb{Z}$. Then $G \cong \mathbb{Z}_9 \times \mathbb{Z}_{11} \cong \mathbb{Z}_{99}$.
   Case 2: $H \cong \mathbb{Z}_3 \times \mathbb{Z}_3$ then $G \cong \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_1 1 \cong \mathbb{Z}_3 \cong \mathbb{Z}_{33}$.

Lecture 20 (2016–03–02).

Proof of Sylow 2. Fix two Sylow p-subgroups $P, Q \leq G$ such that $|P| = |Q| = p^k$. Let $X = G/P$ and let $Q \curvearrowright X$ by left multiplication, i.e., $\forall h \in Q : h \cdot (gP) = (hg)P$.
Note that $|X| = \frac{p^k m}{p^k} = m \not\equiv 0 \pmod p$. Since Q is a p-group, by Fixed-Point Lemma, the number of fixed points is equivalent to $|X| \bmod p$, so we can choose a fixed point $gP \in X$.
We know that for any $h \in Q, h \cdot (gP) = gP$, so $(hg)P = gP$, meaning $g^{-1}hg \in P$.
As $h \in Q$ was arbitrary, $g^{-1}Qg \subseteq P$. As $|g^{-1}Qg| = |P| = p^k$, it follows that $g^{-1}Qg = P$. □

We prove both parts of Sylow 3 separately, as they are somewhat dissimilar

Proof of Sylow 3 (a). Let $X = \{H \leq G : |H| = p^k\}$ be the set of all Sylow p-subgroups of G. so $|X| = n_p$. Let $G \curvearrowright X$ by conjugation, i.e., $g \cdot H = gHg^{-1}$. For convenience, fix some designated Sylow p-subgroup $P \in X$ (which exists by Sylow 1).
This time we're going to use the Orbit-Stabilizer Theorem
By Sylow 2, we know that $\mathcal{O}_P = X$, so $|\mathcal{O}_P| = n_p$. By the Orbit-Stabilizer Theorem, we know that $|\mathcal{O}_P| \cdot |G_P| = |G|$, so $n_p = |G|/|G_p|$. Note also that $|G| = p^k m$.
Note that $P \leq G_P$ since $\forall g \in P, gPg^{-1} = P$. So, by Lagrange's Theorem, we know that $|P|$ divides $|G_P|$, so say $|G_p| = p^k \ell$. Thus, $n_p = \frac{p^k m}{p^k \ell} = \frac{m}{\ell}$. This shows that $m = n_p \ell$, meaning that n_p divides m as desired. □

Proof of Sylow 3 (b). Again let $X = \{H \leq G : |H| = p^k\}$ be the set of all Sylow p-subgroups of G. so $|X| = n_p$. Fix $P \in X$ (which exists by Sylow 1). Let $P \curvearrowright X$ by conjugation.
We know that $P \in X$ is a fixed point of $P \curvearrowright X$.

Claim. P is the only fixed point.

Proof (Claim). Suppose $Q \in X$ is a fixed point. Want to show $Q = P$. So, $\forall g \in P\ g^{-1}Qg = Q$, i.e., $P \leq N(Q)$. We also know that $Q \leq N(Q)$. So, P, Q are both Sylow p-subgroups of $N(Q)$. By Sylow 2, $\exists h \in N(G)$ st $Q = h^{-1}Qh = P$. Hence, $Q = P$. □(Claim)

So the number of fixed points of $P \curvearrowright X$ is 1. P is a p-group, so by the Fixed-Point Lemma, we have $n_p = |X| \equiv 1 \pmod{p}$ $\square$(Sylow 3b)

Example. Let's classify all *abelian* groups G with cardinality 108 (up to isomorphism). First we note that $108 = 2^2 \cdot 3^3$
By Sylow 1, there exist $H, K \leq G$ such that $|H| = 2^2$ and $|K| = 3^3$.
Since G is abelian, $H \trianglelefteq G$ and $K \trianglelefteq G$.
Also, $H \cap K = \{e\}$ by Lagrange's Theorem (since $\gcd(2^2, 3^3) = 1$). So by corollary 84, $G \cong H \times K$.
(We write $\mathbb{Z}_n$ for $\mathbb{Z}/n\mathbb{Z}$, although some number theorists would beg to differ.)
First H. H is isomorphic to either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.
Next, K. $|K| = 27$ and it's abelian (because it's a subgroup of G.)
Case 1 ($\exists k \in K$ such that $|k| = 27$):
In this case, $K \cong \mathbb{Z}_{27}$
Case 2 (No element of order 27, but $\exists k \in K$ such that $|k| = 9$):
We posit that we may take $g \in K/\langle k \rangle$ with $|g| = 3$. (Existance left as an exercise to the reader).
$\langle g \rangle \cap \langle k \rangle = \{e\}$. Thus, by corollary 84, $K \cong \mathbb{Z}_9 \times \mathbb{Z}_3$
Case 3 (All elements have order 3):
Exercise: use Sylow's theorem to show $K \cong (\mathbb{Z}_3 \times \mathbb{Z}_3) \times \mathbb{Z}_3$
These cases are exhaustive, so we have 6 options.
Thus, G could be isomorphic to the direct product of any tuple in $\{\mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2\} \times \{\mathbb{Z}_{27}, \mathbb{Z}_9 \times \mathbb{Z}_3, \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3\}$

Cool note: we won't get to this, but every finite abelian group is isomorphic to the direct product of a direct product of cyclic groups.

Ring Theory

Lecture 21 (2016–03–14).

Definition 94. A ring is a set R equipped with the binary operations $+$ and $\times$ such that the following axioms are true:

(1) $(R, +)$ is an abelian group
(2) $\times$ is associative over R
(3) $\times$ distributes over $+$ i.e., $a\times(b+c) = (a\times b)+(c\times d)$, also, $(a+b)\times c = (a\times c)+(b\times c)$

Notation. We follow the following conventions:

- We usually don't write $\times$. Instead we write expressions like $(a \times b) + c$ as $ab + c$.
- The ring R has the additive identity 0.
- we denote the additive inverse of an element $b \in R$ by $-b$

Definition 95. A ring R is commutative if $\times$ is commutative $(\forall a, b \in R(a \times b = b \times a))$

Definition 96. The ring R has an identity (or a 1) if $\exists 1 \in R(\forall a \in R(1a = a1 = a))$

Remark. If R has a 1, then it is unique. Why? If $1, e$ are both $\times$ identities, then $1 = 1e = e$.

Definition 97. If R has a 1 with $1 \neq 0$ we say R is a division ring if $(R \setminus \{0\}, \times)$ is also a group. (i.e., for all $a \in R, a \neq 0(\exists b \in R), b \neq 0$ st $ab = ba = 1$ $(b = \frac{1}{a})$)

Definition 98. R is a field if it is a commutative division ring.

Example. $\mathbb{Q}$ is a field

Proposition 99. *Let R be a ring. Then $\forall a \in R, 0a = a0 = 0$.*

Proof.

$$0 = 0 + 0$$

Multiply by a

$$0a = (0 + 0)a = 0a + 0a$$

Add $-0a$ to both sides

$$0 = 0a$$

□

Remark. If R has a 1 with $1 = 0$ then $R = \{0\}$. Why? $\forall a \in R, a = 1a = 0a = 0$.

Proposition 100.

(1) $(-a)b = a(-b) = -(ab)$
(2) $(-a)(-b) = ab$
(3) If $1 \in R$ *then* $-a = (-1)a$

Proof. To show $(-a)b = -(ab)$ we check $(-a)b + ab = 0$.
$(-a)b + ab = (-a + a)b = 0b = 0$. Thus, $(-a)b = -(ab)$.
The rest are left as an exercise. □

Definition 101. R is a ring, $a \in R$ is a zero-divisor if:

(1) $a \neq 0$
(2) $\exists b \neq 0$ such that $ab = 0$ or $ba = 0$

Definition 102. R ring with a $1 \neq 0$, $u \in R$ is a unit if $\exists v \in R$ such that $uv = vu = 1$.

Remark. Denote by $R^\times$ the set of units. Then $(R^\times, \times)$ forms a group.

Remark. Since $0 \neq 1$ 0 is never a unit since $0v = 0 \neq 1$.

Proposition 103. *No zero-divisor is a unit*

Proof. Towards a contradiction, suppose $a \neq 0$ is both a zero-divisor and a unit. Fix $b \neq 0$ and $v \in R$ such that $ab = 0$ and $va = 1$ (if $ba = 0$ use $av = 1$) $b = 1b = (va)b = vab = v(ab) = v0 = 0$ So $b = 0$ contradiction □

Example.

(1) $(\mathbb{Z}, +, \times)$ with the usual $+$ and $\times$ is a commutatve ring with a $1 \neq 0$. $\mathbb{Z}$ has no 0-divisors. The units are $\mathbb{Z}^\times = \{1, -1\}$.
(2) $\mathbb{Q}$ are a commutative ring with a $1 \neq 0$. $\mathbb{Q}$ has no 0-divisors. The units are $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$. So $\mathbb{Q}$ is a field.
(3) $R = \mathbb{Z}/n\mathbb{Z}$ with modular arithmetic and $\overline{a} \times \overline{b} = \overline{ab}$. If $n > 1$ then R is a ring. R has a 1, namely $\overline{1}$. $\overline{1} \neq \overline{0}$. Commutative.

   Claim (C1). Suppose $\overline{a} \neq \overline{0}$ with $\gcd(a, n) = d \neq 1$. Then, $\overline{a}$ is a zero-divisor.

   Pf of C1. Choose $b = \frac{n}{d}$ such that $0 < b < n$. So $\overline{b} \neq \overline{0}$. But $\overline{a}\overline{b} = \overline{\left(\frac{a}{d} \times d\right) \times \frac{n}{d}} = \overline{\frac{a}{d} \times n} = \overline{0}$. □(C1)

   Claim (C2). Suppose $\overline{a} \neq \overline{0}$ with $\gcd(a, n) = 1$. Then a is a unit.

   Pf of C2. Fix $x, y \in \mathbb{Z}$ such that $ax + ny = 1$. $\overline{xa} = \overline{ax} = \overline{ax} = \overline{1} \pmod{n}$ □(C2)

   Corollary 104. *If p prime then $\mathbb{Z}/p\mathbb{Z}$ is a field because everything is relatively prime to p.*

Lecture 22 (2016–03–16).

Digression

This is simply a digression. You are *not* responsible for this material.
Can we "test" whether two groups are isomorphic? What is "group data?" Typically, in practice, it's some sort of combinatorial presentation. We realize groups as words in some (typically finite) alphabet with "substitution rules." (Relations to automata theory.) Letters are usually called generators, substitution rules called relations, the entire thing is called a presentation.
Typical data: List of letters and substitution rules $\langle \underbrace{x, y, z, \dots}_{\text{letters}} | \underbrace{x^2 = \epsilon, yzy = z^2, \text{etc...}}_{\text{rules}} \rangle$.
The group action is typically concatenation (also allowing "inverses" of letters).

Example.

- $G = \langle x | \cdot \rangle \cong \mathbb{Z}$
- $G = \langle x | x^n = \epsilon \rangle \cong \mathbb{Z}/n\mathbb{Z}$
- $G = \langle x, y | xy = yx \rangle \cong \mathbb{Z} \times \mathbb{Z}$ $(a, b) \mapsto x^a, y^b$ is an isomorphism
- $G = \langle x, y | x^2 = \epsilon, y^m = \epsilon, yx = xy^{-1} \rangle \cong D_{2m}$. $(x^i y^j)(x^k y^\ell) = x^? y^?$
- $G = \langle x, y | x^2 = \epsilon, y^5 = \epsilon, xyx = y^2, xy^4xy^3x = y^3$ Let's look at y. $y = x^2yx^2 = x(xyx)x = x(y^2)x = xyyx = xyx^2yx = (xyx)(xyx) = y^4 = y^2yy = y^2y^4y^4 = y^{10} = (y^5)^2 = \epsilon$ We also know that $\epsilon = y^3 = x\epsilon x\epsilon x = x^3 = xx^2 = x$. Thus, $G \cong \{e\}$.

Theorem (Novikov, Adyan-Rabin)**.** *There is no computer program which upon input some presentation of a group correctly answers* $G \overset{?}{\cong} \{e\}$.

Proof. Reduce to halting problem. □

The best know algorithm for testing isomorphism given the multiplication table is $\mathcal{O}(n^{\frac{1}{2}\log n})$
Now, back to ring theory.

Example.

4 $\mathbb{Q}[\sqrt{-5}]$ = elements that look like $a + b\sqrt{5}, a \in \mathbb{Q}, b \in \mathbb{Q}$.
$(a + b\sqrt{-5}) + (c + d\sqrt{-5}) = (a + c) + (b + d)\sqrt{-5}$
$(a + b\sqrt{-5}) \times (c + d\sqrt{-5}) = (ac - 5bd) + (ad + bc)\sqrt{-5}$
It's a ring because $0 = 0 + 0\sqrt{-5}$
$1 = 1 + 0\sqrt{-5}$.
$1 \neq 0$
It's also commutative (check left to reader).
Every non-zero element is a unit (u is a unit iff $\exists v(uv = vu = 1)$)
$(a + b\sqrt{-5}) \left(\frac{a - b\sqrt{-5}}{a^2 + 5b^2}\right)$

5 $\mathbb{Q}[x]$ = polynomials of x with rational coefficients. Typical elements are $p(x) = 5, q(x) = x - 7, r(x) = x^{17} - \frac{2}{3} + \frac{1}{7}$. $+, \times$ as usual. Checking the other ring properties left as an exercise.

Polynomials have no zero divisors. $p(x)q(x) = 0 \iff p(x) = 0$ or $q(x) = 0$. Takes a little bit of work to show.

x is *not* a unit. No solution to $xp(x) = 1$ (can formalize by looking at the degree of each side).

6 2×2 matrices over $\mathbb{Q}$. $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, $a, b, c, d \in \mathbb{Q}$ with normal $+, \times$. *Not* commutative ($AB \neq BA$) in general. $\mathsf{0} = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, $\mathsf{1} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

Claim (1). If $\det A \neq 0$ then A is a unit.

Proof. $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), A^{-1} = \frac{1}{\det A}\left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$. □

Claim (2). If $\det A = 0$ then A is a zero-divisor.

Proof. $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right) = \mathsf{0}$ □

Definition 105. If R is a ring which

(1) is commutative
(2) has a $1 \neq 0$
(3) has no zero-divisors

then we say R is an integral domain (abbr. ID). (note: integral means like the integers, not like in calculus.)

Proposition 106. *Suppose R is an ID, $a, b, c \in R$ such that $a \neq \mathsf{0}$ and $ab = ac$. Then $b = c$.*

Proof. $0 = ab - ac = a(b - c)$. Since a is not a zero-divisor (because R is an ID) we know that $b - c = 0$ Thus, $b = c$ as desired. □

Remark. "There's a result that says every finite integral domain is a field, but I don't think we need that"

Definition 107. If $(R, +, \times)$ is a ring and $S \subseteq R$, we say that S is a subring if $(S, +, \times)$ is a ring with the same operations. (In particular, $(S, +) \leq (R, +)$.)

Definition 108. If $(R, +_R, \times_R), (S, +_S, \times_S)$ are rings, we say that $\varphi : R \to S$ is a ring homomorphism (or just homomorphism if "ring" is clear from the context) if for all $r_1, r_2 \in R$:

- $\varphi(r_1 +_R r_2) = \varphi(r_1) +_S \varphi(r_2)$
- $\varphi(r_1 \times_R r_2) = \varphi(r_1) \times_S \varphi(r_2)$

Lecture 23 (2016–03–18).

Class Note

Midterm 2 will be in three weeks: April 8th or 11th.
There will be both group theory and ring theory.

Property 109 (Subring Criteria)**.** Suppose $(R, +, \times)$ is a ring. Then $S \subseteq R$ is a subring iff it satisfies the following properties:

- Non-emptiness
- Closure under $+$
- Closure under $-$
- Closure under $\times$

Note that if we already know that $(S, +) \leq (R, +)$, then we only need to check closure under $\times$.

Example. $5\mathbb{Z}$ is a subring of $\mathbb{Z}$. Already checked $(5\mathbb{Z}, +) \leq (\mathbb{Z}, +)$. Closure under $\times$: Suppose $5m, 5n \in 5\mathbb{Z}$. Then $(5m)(5n) = 25mn = 5(5mn) \in 5\mathbb{Z}$.

Example. $\mathbb{Z}/5\mathbb{Z}$ is *not* a subring of $\mathbb{Z}$.
Note that it's not even a subgroup of $\mathbb{Z}$ (with the operation of addition)

Example (Non-example). $\varphi : \mathbb{Z} \to \mathbb{Z}$, $z \mapsto 2z$. Is *not* a homomorphism. $\varphi(1 \times 1) = \varphi(1) = 2 \neq 4 = 2 \times 2 = \varphi(1) \times \varphi(1)$ (In fact the only two homomorphism $\mathbb{Z} \to \mathbb{Z}$ are $z \mapsto z, z \mapsto 0$)

Example. The map $\varphi : \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}, \varphi(z) = \overline{z} \pmod 3$

Remark. Many authors demand that all rings have a multiplicative identity $\mathsf{1}$. Some of them demand that homomorphisms preserve the $\mathsf{1}$ ($\varphi(\mathsf{1}_R) = \mathsf{1}_S$).

Definition 110. If $(R, +_R, \times_R), (S, +_S, \times_S)$ are rings, define the direct product $(R, +_R, \times_R) \times (S, +_S, \times_S)$ on the set $R \times S$ with $(r, s) + (r', s') = (r +_R r', s +_S s')$ $(r, s) \times (r', s') = (r \times_R r', s \times_S s')$

Example. $\mathbb{Z} \times \mathbb{Z}$ is a ring with $\mathsf{1} = (1, 1)$. The map $\varphi : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}, \varphi(z) = (z, 0)$ is a ring homomorphism., but $\varphi(1) = (1, 0)$ is *not* the identity of $\mathbb{Z} \times \mathbb{Z}$.

Definition 111. $\varphi : R \to S$ is a ring homomorphism. Define the kernel $\operatorname{Ker}(\varphi) \subseteq R$ by $r \in \operatorname{Ker}(\varphi) \iff \varphi(r) = \mathsf{0}_S$

Proposition 112. *Suppose $\varphi : R \to S$ is a ring homomorphism. Put $K = \operatorname{Ker}(\varphi)$. Then:*
(A) K is a subring of R
(B) $\forall a \in K, \forall r \in R(ar \in K \wedge ra \in K)$ (because $\varphi(ar) = \varphi(a)\varphi(r) = 0\varphi(r) = 0$)

Proof of (A). We already know that $(K, +) \leq (R, +)$. Thus, we only need to check closure under $\times$. Fix $a, b \in K$ sp $\varphi(a) = \varphi(b) = 0$. Want $ab \in K$ $\varphi(ab) = \varphi(a)\varphi(b) = 0 \cdot 0 = 0$. Thus $ab \in K$, as desired. □

Definition 113. Let R be a ring, $I \subseteq R$. We say I is an ideal of R if:

(1) I is a subring of R
(2) $\forall r \in R(rI \subseteq I \wedge Ir \subseteq I)$ Where $rI = \{ra : a \in I\}$ and $Ir = \{ar : a \in I\}$

Proposition 114. *If $\varphi : R \to S$ is a ring homomorphism then $\operatorname{Ker}(\varphi)$ is an ideal of R.*

Proposition 115 (Ideal Criteria)**.** *If $I \subseteq R$, R is a ring then I is an ideal iff:*

(1) $I \neq \emptyset$
(2) $\forall a, b \in I(a + b \in I)$
(3) $\forall a \in I(-a \in I)$
(4) $\forall a \in I(\forall r \in R(ar \in I \wedge ra \in I))$

(Note that the last criterion is stronger than closure under $\times$ in I.)

Example. $5\mathbb{Z}$ is an ideal of $\mathbb{Z}$.
We've already checked it's a subring. Fix arbitrary $5m \in 5\mathbb{Z}$ and $z \in Z$. Then $(5m)z = 5(mz) \in 5\mathbb{Z}$. $z(5m) = 5(zm) \in 5\mathbb{Z}$. Thus, as our choices were arbitrary, $5\mathbb{Z}$ is an ideal

Example (Non-example). $R = 2 \times 2$ matrices with entries in $\mathbb{Q}$. $I = \{A \in R : \det A = 0\}$ Note that it satisfies the last ideal criterion. However, it is not closed under addition. $\left(\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) = I_2$ and $\det I_2 \neq 0\right)$

Definition 116. If R is a ring, I is a subring, define $R/I = \{r + I : r \in R\}$ (this is exactly $(R, +)/(I, +)$).

Note $(r + I) + (s + I) = (r + s) + I$ is a well-defined abelian group operation on R/I.

Proposition 117. *If I is an ideal of R, the map $(r+I)(s+I) = rs+I$ is well-defined.*

Proof. Suppose $r+I = r'+I$ $(r-r' \in I)$, $s+I = s'+I$ $(s-s' \in I)$
Want to show that $rs+I = r's'+I$ (i.e., $rs-r's' \in I$)
$rs - r's' = rs + (-rs' + rs') - r's' = \underbrace{r(s-s')}_{\in I} + \underbrace{(r-r')s'}_{\in I} \in I$ □

Lecture 24 (2016–03–21). First, we're going to look at the ring-theoretic equivalent of the first isomorphism theorem.

Proposition 118. *Suppose R, S are rings, $\varphi : R \to S$ is a (ring) homomorphism. Then $\mathrm{Im}(\varphi) = \{s \in S : \exists r \in R(\varphi(r) = s)\}$ is a subring of S.*

Proof. We already know that $(\varphi[R], +) \leq (S, +)$. So, $\varphi[R] \neq \emptyset$, and it's closed under $+$ and $-$.
Thus, we only need to check closure under $\times$. Fix $s_1, s_2 \in \varphi[R]$. Fix r_1, r_2 with $\varphi(r_i) = s_i$.
Want $s_1 s_2 \in \varphi[R]$.
Check $\varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2) = s_1 s_2$. Thus, $s_1 s_2 \in \varphi[R]$. □

Definition 119. A (ring) isomorphism is a bijective (ring) homomorphism. If $\exists \varphi : R \to S$ an isomorphism, then we write $R \cong S$.

Theorem 120 (First Isomorphism Theorem for Rings)**.** *. Suppose $\varphi : R \to S$ is a ring homomorphism. Then $R/\ker(\varphi) \cong \varphi[R]$.*

Proof. Put $K := \ker(\varphi)$ By First Isomorphism Theorem, the map $\Psi : R/K \to \mathrm{Im}(\varphi)$ with $\Psi(r+K) = \varphi(r)$ is a bijective group homomorphism from $(R/K, +)$ to $(\mathrm{Im}(\varphi), +)$. To verify that Ψ is a ring isomorphism, we just need it to preserve $\times$.
Fix $r_1 + K, r_2 + K \in R/K$. $\Psi((r_1+K)(r_2+K)) = \Psi(r_1 r_2 + K) = \varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2) = \Psi(r_1+K)\Psi(r_2+K)$ □

Ideals are the same thing as kernels of homormorphisms.
More on ideals:

Proposition 121. *If $I, J \subseteq R$ are ideals, then $I \cap J$ is an ideal.*

Proof. See Homework 7. □

Proposition 122. *If $I, J \subseteq R$ are ideals, then $I + J = \{i + j : i \in I, j \in J\}$ is an ideal.*

Proof. We need to check our ideal criteria.
Non-zero: $0 = 0 + 0 \in I + J$.
Closed under $+$: Fix $i + j, i' + j' \in I + J$. Then $(i+j) + (i'+j') = (i+i') + (j+j') \in I + J$
Closed under $-$: Fix $i + j \in I + J$. Then $-(i+j) = (-i) + (-j) \in I + J$
Closed under $\times$ by R: Fix $i + j \in I + J$ and $r \in R$. Then $r(i+j) = ri + rj \in I + J$ and $(i+j)r = ir + jr \in I + J$ □

Definition 123. Fix an $a \in R$, R a ring. Let (a) denote the smallest ideal containing a. I.e., (a) is the intersection of all ideals containing a. We call (a) the principal ideal generated by a.
If $A \subseteq R$ we denote by (A) the smallest ideal containing all elements of A. I.e.,

$$(A) = \bigcap_{\substack{I \text{ an ideal} \\ I \supseteq A}} I.$$

Remark. $I + J = I \cup J$

Proposition 124. *Suppose R is a commutative ring with a 1.*
Then $(a) = aR = \{ar : r \in R\}$. $(a) = R$ iff a is a unit.

Proof. First show $aR \subseteq (a)$:
Fix $r \in R$. We know $a \in (a)$ So $ar \in (a)$. Hence $aR \subseteq (a)$.
Next show $aR \supseteq (a)$:
Since (a) is the "smallest" ideal containing a, it suffices to check that aR is an ideal containing a.

(1) $(a \in aR)$: $a = a \cdot 1 \in aR$ (used that $1 \in R$).
(2) (aR is nonempty): $0 = a0 \in aR$
(3) (Closure under $+$): $ar_1 + ar_2 = a(r_1 + r_2) \in aR$
(4) (Closure under $-$): $-(ar) = a(-r) \in aR$
(5) (Closure under $\times$ by R): Fix $ar \in aR, s \in R$ First $(ar)s = a(rs) \in aR$. Second, $s(ar) = a(sr) \in aR$ (uses commutativity).

□

Remark. If R is not commutative but it still has a 1, we have if a is a unit then $(a) = R$. Otherwise, $(a) = \{\sum_{i=1}^{k} r_i a s_i : r_i, s_i \in R, k \in \mathbb{Z}^+\}$.

Remark. Warning: if R has no 1, then typically (a) is much bigger than aR (or RaR). For example, $R = 5\mathbb{Z}, a = 10$, $(a) = 10\mathbb{Z}$ but $aR = \{\ldots, -100, -50, 0, 50, 100, \ldots\}$.

Proposition 125. *Suppose R has a 1. $I \subseteq R$ is an ideal. Then $I = R$ iff I contains a unit. (So $(u) = R$ iff u is a unit).*

Proof. ($\Longrightarrow$): Assume $I = R$. Then $1 \in I$.
($\Longleftarrow$): Suppose $u \in I$, u a unit. $\exists v \in R$ such that $uv = 1$. $1 = uv \in I$. Now fix $r \in R$. Then, $r = 1 \cdot r \in I$, so $I = R$ as desired. □

Corollary 126. *Suppose R is a commutative ring with $1 \neq 0$. Then R is a field if its only ideals are $(0) = \{0\}$ and R.*

Proof. ($\Longrightarrow$): Suppose R is a field and $I \subseteq R$ is an ideal. If $I = \{0\}$ then we're done. Otherwise, $\exists r \neq 0$ with $r \in I$. Since r is a unit, $I = R$.
($\Longleftarrow$): Suppose R has only $\{0\}$ and R for its ideals. Fix $0 \neq r \in R$. Want to show that r is a unit. Look at (r). We know $r \in (r)$, so $r \neq 0$. Hence $(r) = R$. We also know that $(r) = rR$ by our assumptions along with proposition 125. So, $\exists s \in R$ such that $rs = 1$. We also have $sr = 1$. Thus r is a unit. □

Lecture 25 (2016–03–23).

"When you're a professor you don't make mistakes, you make teachable moments."

Definition 127. If $f : X \to Y, A \subseteq X, B \subseteq Y$, $f^{-1}[B] = f^{-1}(B) = \{x \in X : f(x) \in B\}$.

Proposition 128. *Suppose $\varphi : R \to S$ is a ring homomorphism with $B \subseteq S$ then,*

(1) B is a subring of $S \implies \varphi^{-1}[B]$ is a subring of R.
(2) B is an ideal of $S \implies \varphi^{-1}[B]$ is an ideal of R.

The proof is left as an exercise.

Proposition 129. *If $\varphi : R \to S$ is a surjective ring homomorphism, and $I \subseteq R$ is an ideal, then $\varphi[I] \subseteq S$ is an ideal of S.*

The proof is left as an exercise.

Definition 130. An ideal $I \subseteq R$ is a proper ideal if $I \neq R$.

Definition 131. An ideal $M \subseteq R$ is a maximal ideal if:

(1) M is proper
(2) If I is a proper ideal with $M \subseteq I$, then $I = M$.

Remark ((s)).
- The zero ring $R = \{0\}$ has no proper ideals. Hence, it has no maximal ideal.
- If R is a commutative ring with a $\mathsf{1}$, then R is a field iff $\{0\}$ is maximal.
- Fact/Axiom If R has a $\mathsf{1}$ then every proper ideal is contained in a maximal ideal. (This requires set theory). (We'll never actually use this in class probably).

Proposition 132. *Suppose R is a commutative ring with a $\mathsf{1}$ and $M \subseteq R$ is an ideal. Then M is maximal iff R/M is a field.*

Proof. ($\Longrightarrow$)
Take M to be a maximal ideal. Since M is proper, $\mathsf{1} \notin M$. Hence in R/M we have $1 + M \neq 0 + M$.
Just need to show that the only ideals of R/M are $\{0 + M\}$ and R/M.
Suppose $I \subseteq R/M$ is an ideal. Fix $\varphi : R \to R/M$ to be the "quotient homomorphism" $\varphi(r) = r + M$.
$\varphi^{-1}[I]$ is an ideal in R. Moreover. if $m \in M$ then $\varphi(m) = m + M = \mathsf{0} + M \in I$. So, $M \subseteq \varphi^{-1}[I]$. Now we can use maximality. Since M is maximal, there are two options for $\varphi^{-1}[I]$.
If $\varphi^{-1}[I] = M$ then $I = \{0 + M\}$.
If $\varphi^{-1}[I] = R$ then $I = R/M$.
Thus, R/M is a field.
($\Longleftarrow$) (Sketch) R/M is a field and $M \subseteq I \subseteq R$, with I an ideal. Look at $\varphi[I] = \{\mathsf{0} + M\}$ or R/M. (Full proof is left as an exercise). □

Definition 133. R is a commutative ring with a $\mathsf{1}$. An ideal $P \subseteq R$ is a prime ideal if:

(1) P is proper
(2) $\forall a, b \in R$, if $ab \in P$ then either $a \in P$ or $b \in P$

Proposition 134. *Let R be a commutative ring with a $\mathsf{1}$, and $P \subseteq R$ is an ideal. Then P is prime iff R/P is an integral domain.*

Proof (Sketch). ($\Longrightarrow$) P prime, want R/P to be an integral domain. Toward a contradiction, suppose that $r + P, s + P \neq \mathsf{0} + P$ with $rs + P = (r + P)(s + P) = 0 + P$. I.e., $rs \in P$. As P is prime, one of r, s is in P. If $r \in P$ then $r + P = \mathsf{0} + P$, contradiction. By symmetry, $s \in P$ is also a contradiction.
($\Longleftarrow$) Similar. □

Corollary 135. *If R is a commutative ring with a $\mathsf{1}$ and $I \subseteq R$ is an ideal, then I is maximal $\implies$ I is prime.*

Proof. If R/I is a field, it's an integral domain. Then simply apply the previous proposition. □

Example. Examples in $\mathbb{Z}$:

- Every ideal of $\mathbb{Z}$ is principal.
- Every subgroup of $(\mathbb{Z}, +)$ has the form $n\mathbb{Z} = (n)$ for some $n \in \mathbb{N}_0$.
- Which of the (n) are prime? Answer: when n is prime or zero.
  If p is prime, then $z \in (p)$ iff $p|z$. So, $ab \in (p) \implies a \in (p)$ or $b \in (p)$ If $n \neq 0$ is composite, say $n = ab$. $ab \in n, a \notin (n), b \notin (n)$
- Which (n) are maximal?
  If (n) it is prime, so $n = 0$ or n is a prime number. (0) is not maximal (as $(0) \subsetneq (2) \subsetneq \mathbb{Z}$).
  If p is prime, then (p) is maximal. Why? Fix $a \notin (p)$. Show that $(\{p, a\}) = \mathbb{Z}$ (where $(\{p, a\})$ is the ideal generated by the set $\{p, a\}$) Since $\gcd(p, a) = 1$ fix $x, y \in \mathbb{Z}$ such that $px + ay = 1$. $px = ay$ is in any ideal containing both p and a. So, $1 \in (\{p, a\})$. Hence $(\{p, a\}) = \mathbb{Z}$.
- So in $\mathbb{Z}$, nonzero prime ideal $\iff$ maximal ideal
- Bonus facts: Suppose $a, b, c \in \mathbb{Z}$ all non-zero.
  - If $(c) = (a) \cap (b) \iff \operatorname{lcm}(a, b) = c$
  - $(c) = (a) + (b) \iff \gcd(a, b) = c$

Lecture 26 (2016–03–25).

Class Note

Exam 2 will be on Monday April 11th
(Also HW 9 is posted, don't forget they mention that R has a $1 \neq 0$)

Definition 136. If R is a commutative ring, $R[x]$ = polynomials with coefficients in $R = \sum_{i=0} a_i x^i$. (Note that if R has no 1 then x^0 doesn't exists so just write it as $a_0 + \sum_{i=1} a_i x^i$).

Property 137.

$$\left(\sum_{k=0}^{m} a_k x^k\right) \times \left(\sum_{k=0}^{n} b_k x^k\right) = \sum_{k=0}^{m+n} \left(\left(\sum_{i=0}^{k} a_i b_{k-i}\right) x^k\right)$$

Last time: we showed that given a commutative ring R with a 1, and an ideal $I \subseteq R$.

- I is maximal $\iff$ R/I is a field.
- I is prime $\iff$ R/I is an ID.

The first point generalizes $(\mathbb{Z}/p\mathbb{Z})$ is a field for prime p. The "other" way to make a field out of $\mathbb{Z}$ is "$\mathbb{Q}$."

Field of Fractions

Theorem 138. *Suppose $R \neq \{0\}$ is a commutative ring with no zero-divisors. Then there is a field Q with a subring $R' \subseteq Q$ with $R \cong R'$*

Proof (sketchy). [2]

[2]Side note to the reader: if you've ever constructed the rationals from the integers before, we'll be following approximately that sort of procedure.

Put $D := R \setminus \{0\}$. D satisfies:

- $D \neq \mathsf{0}$ (because $R \neq \{\mathsf{0}\}$)
- $\mathsf{0} \notin D$
- D contains no zero-divisors
- $\forall a, b \in D (ab \in D)$

D will be the set of valid "denominators" in our construction.
Formally define $F = R \times D = \{(r, d) : r \in R, d \in D\}$.
Think of (r, d) as "$\frac{r}{d}$".
Define $\approx$ on F by $(r, d) \approx (s, e) \iff re = sd$.
Exercise: Prove that $\approx$ is an equivalence relation.
Denote by Q the set $F/\approx$ of equivalence classes of $\approx$.
Write $\frac{r}{d}$ for the equivalence class $[(r, d)]_\approx$.
So, $\frac{r}{d} = \frac{s}{e} \iff (r, d) \approx (s, e) \iff re = sd$.
Formally "define" addition and multiplication in Q by

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd} \qquad\qquad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$$

Note that $bd \in D$ because D is closed under multiplication.

Claim (1). Addition in Q is well-defined

Proof that addition is well defined (C1). We need to show if $\frac{a}{b} = \frac{a'}{b'}$, $\frac{c}{d} = \frac{c'}{d'}$ (i.e., $ab' = a'b$ and $cd' = c'd$), then $\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$. I.e., $\frac{ad+cb}{bd} = \frac{a'd'+c'b'}{b'd'}$, i.e., $(ad + cb)b'd' = (a'd' + c'b')bd$.

$$\begin{aligned}(ad + cb)b'd' &= adb'd' + cbb'd' \\ &= (ab')dd' + (cd')bb' \\ &= (a'b)dd' + (c'd)bb' \\ &= a'd'bd + c'b'bd \\ &= (a'd' + c'b')bd\end{aligned}$$

□

Claim (2). Multiplication in Q is well-defined

Proof that multiplication is well defined (C2). The proof is left as an exercise to the reader. □(C2)

Claim (3). $(Q, +, \times)$ is a ring

Proof of Claim 3. $(Q, +)$ is an abelian group as we already know that $+$ is commutative and associative.

Subclaim. $\forall d, d' \in D$, $\frac{\mathsf{0}}{d} = \frac{\mathsf{0}}{d'}$.
Pf (subclaim). $\mathsf{0}d' = \mathsf{0} = \mathsf{0}d$ □

Let $\mathsf{0}_Q$ denote the unique element of Q of the form $\frac{\mathsf{0}}{d}$ for $d \in D$. Check: $\frac{\mathsf{0}}{d} + \frac{a}{b} = \frac{0b+ad}{db} \stackrel{?}{=} \frac{a}{b}$
Note that $adb = abd$, so the final equality holds.
Thus, $\frac{\mathsf{0}}{d} = \mathsf{0}_Q$ is the additive identity.
We assert that $-\left(\frac{a}{b}\right) = \frac{-a}{b}$.

Next, we show that $\times$ is an associative binary operator on Q and that the distributive property holds.

Fire Alarm

Unfortunately at this point, the fire alarm went off. It is left to the reader to complete the proof or look up the remainder of it in the textbook.

□

□(Thm)

Lecture 27 (2016–03–28).

Polynomials Over Integral Domains

First, we're going to focus on polynomials over fields. Typical polynomial in $R[x]$ looks like $p(x) = \sum_k^n a_k x^k$ with $a_k \in R$ and $n \in \mathbb{N}_0$.
Questions: Can we factor them? Uniquely? Can we "solve" polynomial equations, etc.

Definition 139.

- Each a_k is a coefficient
- Each $a_k x^k$ is a term
- The largest k with $a_k \neq 0$ (if it exists) is called the degree of $p(x)$ (denoted $\deg p$)
- If all $a_k = 0$ we leave the degree undefined (but we can consider it to be $-\infty$ for various reasons that "we're not going to get into")
- If $\deg p = n$ we call $a_n, a_n x^n$ the leading coefficient and the leading term, respectively.
- If the leading coefficient is 1, we say p is monic.

Proposition 140. *Let R be an integral domain, $p(x), q(x) \in R[x]$ both non-zero. Then,* $\deg(p(x)q(x)) = \deg p + \deg q$.

Proof. Suppose $\deg p = m, \deg q = n$. Apply the definition of multiplication. The leading term of the products is therefore $a_m b_n x^{m+n}$. ($a_m b_n \neq 0$ because R is an integral domain). □

Corollary 141. *R is an integral domain.*

(1) Units of $R[x]$ are exactly the units of R (viewed as a degree 0 polynomial.)
(2) $R[x]$ is an ID.

Proof.

(1) Suppose p is a unit. Fix $q \in R[x]$ such that $p(x)q(x) = 1$. $\deg(1) = 0$. So, $\deg(pq) = \deg(p) + \deg(q) = 0$ Hence, $\deg p = \deg q = 0$. Thus, $p(x) = a_0, q(x) = b_0$. $a_0 b_0 = 1$, so a_0, b_0 are units in R.
(2) Analogous.

□

Theorem 142 (Division Algorithm for Polynomials over fields)**.** *Suppose F is a field, $a(x), b(x) \in F[x]$ with $b(x) \neq 0$. Then, there are $q(x), r(x) \in F[x]$ such that*

- $a(x) = q(x)b(x) + r(x)$
- $r = 0$ *or* $\deg r < \deg b$

(Also q and r are unique, proof left as an exercise.)

Proof. We proceed by induction on $m = \deg a$.
If $a = 0$, then $q = r = 0$.
Suppose the theorem is true for all a' (with the same b) with $\deg(a') < m$.
Case 1 ($\deg a < \deg b$):
$a = 0b + a$
Case 2 ($\deg a \geq \deg b$):
Denote by n the degree of b. Fix leading terms $a_m x^m$ of $a(x)$ and $b_n x^n$ of $b(x)$.
Define $a'(x) = a(x) - \frac{a_m}{b_n} x^{m-n} b(x)$.

Claim. $\deg a' < \deg a$ (or $a' = 0$)

Proof (Claim). Coefficients above m are 0. What about the coefficient of x^m? It equals $a_m - \frac{a_m}{b_n} b_n = 0$.
So, $\deg(a') < n$ (or $a' = 0$) □

So, by induction, $\exists q', r' \in F[x]$ such that
- $a'(x) = q'(x)b(x) + r'(x)$
- $r' = 0$ or $\deg r' < \deg b$

We know

$$\begin{aligned} a(x) &= a'(x) + \frac{a_m}{b_n} x^{m-n} b(x) \\ &= q'(x)b(x) + r'(x) + \frac{a_m}{b_n} x^{m-n} b(x) \\ &= \underbrace{\left(q'(x) + \frac{a_m}{b_n} x^{m-n}\right)}_{q(x)} b(x) + r'(x) \end{aligned}$$

.

□

We needed F to be a field. Consider $a(x) = 3x + 1, b(x) = 2$ in $\mathbb{Z}[x]$.

Definition 143. An ID R is a Euclidean domain (ED) if there is a function $N : R \to \mathbb{N}$ such that $\forall a, b \in R, b \neq 0\ \exists q, r \in R$ with
- $a = qb + r$
- $r = 0$ or $N(r) < N(b)$

Notation. N (as described above) is called a *norm*.
- q is the quotient
- r is the remainder

Example.
- $R = \mathbb{Z}$, $N(z) = \text{abs } z$
- $F[x]$ with F a field, $N(p) = \deg p$
- F a field, N any function.

Definition 144. An ID R, is a principal ideal domain (PID) if every ideal is principal (i.e., $I \subseteq R$ an ideal $\implies \exists a \in R(I = (a) = aR)$)

Proposition 145. *Every Euclidean domain is a principal ideal domain.*

Proof. Fix ED R, $I \subseteq R$ an ideal. If $I = \{0\}$ then $I = (0)$. If $I \neq \{0\}$, fix $a := \arg\min_{a \in I \setminus \{0\}} N(a)$.

Claim. $I = (a)$

Proof of Claim. $(a) \subseteq I$, need $I \subseteq (a)$ Fix $s \in I$. By ED, $\exists q, r \in R$ such that $s = qa + r$ with $N(r) < N(a)$ or $r = 0$. $r = s - qa \in I$. Thus, as a was minimal, $r = 0$. Thus $s = qa \in (a)$ □

□

Lecture 28 (2016–03–30).

Remark. R commutative ring, $a \in R$.
The map $eval_a : R[x] \to R$ $p(x) \mapsto p(a)$ is a homomorphism of rings.

Let's go back to EDs. EDs are PIDs in particular $F[x]$ with F a field.

Example. $\mathbb{Z}[x]$ is *NOT* a PID. We'll show this by contradiction.
Look at $I = \{p(x) \in \mathbb{Z}[x] : \text{ constant term is even}\}$ $I = eval_0^{-1}(2\mathbb{Z})$ hence an ideal. Suppose I were principal, say $I = (p(x))$. First $2 \in I$ (constant 2 polynomial. 2 is a multiple of $p(x)$) $p(x)$ cannot be ± 1 as otherwise $(p(x)) = \mathbb{Z}[x]$ so $p(x) = \pm 2$. We also know $x \in I$. But there is no $q(x)$ such that $x = 2q(x)$. Thus ± 2 can't generate it. Thus I is not principle.
Variant: if $R[x]$ is a PID, then R is a field.

Definition 146. Let R be a commutative ring and $a, b \in R$ we say a divides b, or $a \,|\, b$, if $\exists r \in R(ar = b)$.

Proposition 147. *For $a, b \in R$, R commutative with a $1 \neq 0$, the following are equal:*

(1) $a \,|\, b$
(2) $b \in (a)$
(3) $(b) \subseteq (a)$

Proof. $(1 \implies 2)$:
$a \,|\, b$ $\exists r \in R$ $ar = b$, $ar \in I$ for all ideals I with $a \in I$. Hence $b = ar \in (a)$.
$(2 \implies 3)$:
(a) is an ideal, it contains b. (b) is the smallest such ideal. Thus $(b) \subseteq (a)$.
$(3 \implies 1)$:
$(a) = aR = \{ar : r \in R\}$. $(b) \subseteq (a), b \in (a)$, so $b = ar$ for some $r \in R$.

□

Definition 148. We say $a, b \in R$ (commutative ring with a 1) are commensurate if $(a) = (b)$. (By proposition, $a \,|\, b$ and $b \,|\, a$)

Proposition 149. *Suppose R is an ID. Then, $a, b \in R$ are commensurate iff there exists a unit u such that $a = ub$.*

Proof. (Commensurate $\implies \exists u$):
Fix $r, s \in R$ such that $ar = b$, $bs = a$. So $(ar)s = a \implies a(rs) = a$ So, $a(rs - 1) = 0$ If $a = 0$ then $b = 0$ so $0 = 10$. Otherwise, $rs - 1 = 0 \implies rs = 1$ so s is a unit.
$(\exists u \implies$ commensurate):
Suppose $a = ub$, $b \,|\, a$ u a unit, $\exists v \in R$ $vu = uv = 1$. Hence $va = vub = 1b = b$ Thus $a \,|\, b$.
Hence a, b are commensurate.

□

Definition 150. Work in commutative ring R with a 1. We say d is a gcd of the nonzero elements $a, b \in R$ if

(1) $d|a$ and $d|b$
(2) If $c|a$ and $c|b$ then $c|d$

Note that if d and d' are both gcds of the same pair a, b. $d|d'$ and $d'|d$, so d and d' are commensurate and thus, in an ID, $\exists u$ unit such that $d = ud'$.

Theorem 151. *If R is a principal ideal domain, then gcds exists. (If $a, b \in R$ nonzero, $\exists d \in R$ such that d is a gcd of a, b.) Moreover, this gcd d has the form $d = ax + by$ for some $x, y \in R$.*

Proof. Note that it is enough to show that there exists a gcd of the form $ax + by$
Let I be the ideal $(a) + (b) = \{r + s : r \in (a), s \in (b)\}$.
This ideal is principal as R is a PID, so say $I = (d)$.
$d \in (d)$ so $d = r + s$ for some $r \in (a), s \in (b)$, so $d = ax + by$ for some $x, y \in R$.

Claim. d is a gcd of a, b.

Proof. $a \in (a)$, hence $a = a + 0 \in (a) + (b) = I$. $a \in (d)$, so $d|a$. Similarly, $d|b$. □(Claim)

Next, suppose $c \in R$ such that $c|a$ and $c|b$.
Fix $r, s \in R$ such that $a = rc, b = sc$ $a \in (c), b \in (c)$. Thus, $d = ax+by \in (c)$ so $c|d$. □(Thm)

In particular, polynomials, over a field always have gcds.
Next time we'll prove polynomials admit unique factorizations.

Lecture 29 (2016–04–01).

Class Note

Homework 10 is now due Friday April 8 at any time.
Midterm 2 will still be on Monday April 11.
No homework will be due exam week.

Remark. "Commensurate" also called "associate". Sometimes we'll even write $a \sim b$.

Story so far:

Fields $\subseteq$ Euclidean domains $\subseteq$ Principal ideal domains $\subseteq$ Integral domains

Proposition 152. *Suppose R is a PID and $I \subseteq R$ is a nonzero ideal. Then, I is a prime ideal iff I is a maximal ideal.*

Proof. Maximal $\implies$ Prime (R commutatvive with a $1 \neq 0$) was already done.
Next we want to show Prime $\implies$ Maximal. So suppose I is a nonzero prime. Pick a generator $p \neq 0$ with $I = (p)$. Now suppose J is another ideal with $I \subseteq J \subseteq R$. We want to prove that $J = I$ or $J = R$.
Fix a generator $a \neq 0$for J so that $(a) = J$.
$(p) \subseteq (a)$ so $a|p$ Fix $r \in R$ such that $p = ar$. $ar \in (p) = I$. As I is prime, either $a \in I$, or $r \in I$.
Case 1 ($a \in I$):
This means $(a) \subseteq I$. So $J \subseteq I$, thus $J = I$
Case 2 ($r \in I$):
$r \in (p)$ so $p|r$. Say $r = bp$ for some $b \in R$. $p = ar = abp$. $p - abp = 0$, $(1 - ab)p = 0$.
Thus, $1 - ab = 0$ or $1 = ab \in (a)$. Hence $J = (a) = R$

□

What does (maximal = prime) say about ring *elements*?

Definition 153. Let R be an ID. We say $p \in R$ is prime when:

- $p \neq 0$
- p is not a unit
- $\forall a, b \in R$ if $p|ab$ then $p|a$ or $p|b$.

Exercise. R is an ID. Prove that $p \neq 0$ is prime iff (p) is a prime ideal.

R an ID.

Definition 154. We say that $r = ab$ is a proper factorization if neither a nor b is a unit.

Definition 155. We sat $r \in R$ is irreducible if:

- $r \neq 0$
- r is not a unit
- r admits no proper factorization. ($\forall a, b \in R$, if $ab = r$ then either a or b is a unit)

Proposition 156. *Suppose $r \neq 0$ and $r = ab$ is a proper factorization of r. Then $(r) \subseteq (a) \subseteq R$ and $(a) \neq (r), (a) \neq R$. Particularly, (r) is not maximal.*

Proof. $(r) \subseteq (a) \subseteq R$ is clear since $a|r$.

$(a) \neq (r)$: Towards a contradiction, suppose $(a) = (r)$. So, a, r are associative. Thus, as R is an ID, $\exists$ a unit $u \in R(r = au)$. $a(u - b) = au - ab = r - r = 0$ $a \neq 0$ since $ab = r \neq 0$. So $u - b = 0$, so $b = u$. This is a contradiction since b is not a unit.

$(a) \neq R$: $(a) = R$ would imply a is a unit. But it isn't. □(prop)

Proposition 157. *In a PID $r \neq 0$ is irreducable iff (r) is a maximal ideal.*

Proof. Maximal $\implies$ Irreducible:
Note that (r) maximal means $(r) \neq R$. so r is not a unit. Now suppose r has a proper factorization $r = ab$. We would have $(r) \subsetneq (a) \subsetneq R$. This would contradict maximality. Thus, r has no proper factorization, so it is irreducible.
Irreducible $\implies$ Maximal:
Suppose r is irreducible. Towards a contradiction suppose (r) is not maximal. I.e., $\exists$ an ideal $I \subseteq R$ with $(r) \subsetneq I \subsetneq R$. Since R is a PID, fix $a \in R$ with $(a) = I$. *Check: any facorization $r = ab$ is proper.* This contradicts irreducibility. Hence $r = ab$ is proper. □

Corollary 158. *In a PID, an element r is prime iff r is irreducible.*

Proof. Look at (r). □

Looking back at proving unique factorization of integers, we see that we used primeness coinciding with irreducibility.

Definition 159. A ring R is a Noetherian Ring if there is no strictly increasing sequence $I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \dots$ of ideals.

Proposition 160. *If R is a PID, then R is Noetherian.*

Proof. Towards a contradiction, say we have a sequence $I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \dots$ of ideals.
On Homework: $I = \bigcup_{n \in \mathbb{N}} I_n$ is also an ideal. R is a PID, so I is principal, so $I = (c)$ for some $c \in I = \bigcup_{n \in \mathbb{N}} I_n$. Fix n such that $c \in I_n$. So $(c) \subseteq I_n$. But $I_{n+1} \subseteq \bigcup_{n \in \mathbb{N}} I_n = (c) \subseteq I_n$. Hence $I_n = I_{n+1}$. This is a contradiction, so R is Noetherian. □

Lecture 30 (2016–04–04).

Class Note

This lecture is the cutoff for midterm 2 material. No material after this lecture will be on the exam.

Digression

A tree is a set of nodes (or vertices) with a binary relation "is a child of" such that
- There is a special root node that is the
- Every node but the root node is the child of exactly one other node. (The root is not a child.)
- Every node is a descendant of the root node

Definition 161. y is a descendant of x if:
- $y = x$ or
- y is a child of x or
- y is a child of a child of x or
- ...

Write $\operatorname{desc}(x)$ for the set of descendants of x.

Definition 162. A node is terminal (or is a leaf) if $\operatorname{desc}(x) = \{x\}$

Definition 163. A branch through a tree is a sequence $(x_n)_{n\in\mathbb{N}}$ such that
- x_0 is the root
- x_{n+1} is a child of x_n

Definition 164. A tree is locally finite if every node has finitely many (immediate) children.

Note that a locally finite tree can still have an infinite number of nodes in total.

Lemma 165 (König)**.** *Suppose that T is a locally finite tree with infinitely many nodes. Then T has a branch*

Proof. Note that if x is a node with $\operatorname{desc}(x)$ infinite, then x has a child y with $\operatorname{desc}(y)$ infinite.

$$\operatorname{desc}(x) = \{x\} \cup \bigcup_{i=1}^{n} \operatorname{desc}(y_i)$$

where y_i are the children of x. If all of the $\operatorname{desc}(y_i)$ were finite, $\operatorname{desc}(x)$ would also be finite, so there must be at least one y_i with infinitely many descendants.
Note: The root (by hypothesis) has infinitely many descendants. We build a branch as follows: $x_0 =$ root. Build x_{n+1} a child of x_n such that $\operatorname{desc}(x_{n+1})$ is infinite. □

So how are we going to use König's lemma? Unique factorization!

Theorem 166 (Unique Factorization)**.** *Suppose that R is a Principal Ideal Domain, and $r \in R$ is a non-zero element that is not a unit. Then:*

(1) There exists a sequence $p_1, \ldots, p_m$ of irreducibles in R such that $r = p_1 p_2 \ldots p_m$

(2) This factorization is "unique up to associates" i.e., if $r = q_1 \dots q_n$ is another factorization into irreducibles, then $m = n$ and $\exists \sigma \in S_n$ such that $p_i \sim q_{\sigma(i)}$

Proof.

(1) Build a "factorization tree" T with a root r such that:
- If a node is reducible, it has two children which form a proper factorization
- If a node is irreducible, it is terminal.

Claim. T has no branch.

Proof of claim. If T had a branch, $x_0 = r, x_1, \dots$ then $\forall n \in \mathbb{N}, (x_n) \subsetneq (x_{n+1})$. So $(x_0) \subsetneq (x_1) \subsetneq (x_2) \subsetneq \dots$, is a strictly increasing sequence of ideals of R, contradicting Noetherianness. □(Claim)

Thus, by König's Lemma, the tree is finite. So, the tree lies above some finite level. From here, we see r is the product of the irreducibles on the terminal nodes.

(2) Suppose $r = p_1 p_2 \dots p_m = q_1 \dots q_n$ are factorizations into irreducibles. (Recall that in PIDs, irreducibles $\equiv$ primes.)

We'll proceed by induction on m. (The reader can check $m = 1$.)

We know that $p_m \mid q_1 \dots q_n$ and p_m is prime, so $\exists i \leq n$ such that $p_m \mid q_i$.

Say that $p_m u = q_i$ for $u \in P$. Note that u is a unit. Thus, $p_m \sim q_i$. Also, we have $p_1 p_2 \dots p_m = q_1 \dots \underbrace{(p_m u)}_{=q_i} \dots q_n$. Thus, $p_1 p_2 \dots p_{m-1} = \underbrace{u q_1}_{:=q_1'} \dots q_{i-1} q_{i+1} \dots q_n$.

Now that we've reduced m by 1, induction handles the rest. □(Thm.)

Definition 167. A UFD (Unique Factorization Domain) is an ID satisfying Unique Factorization.

Remark. In UFDs, primeness $\equiv$ irreducibility, in IDs, primeness $\implies$ irreducibility.
Thus, so far,

$$\text{Fields} \subset \text{EDs} \subset \text{PIDs} \subset \text{UFDs} \subset \text{IDs}$$

Corollary 168. *If F is a field, then $F[x]$ is a UFD. Moreover, if $p(x) \in F[x]$ is monic, there is a unique factorization of $p(x)$ into irreducible monic polynomials.*

Lecture 31 (2016–04–06).

Gaussian Integers

$\mathbb{Z}[\mathrm{i}]$, the ring of Gaussian integers.
First, a refresher regarding the complex numbers ($\mathbb{C}$):

Basic properties of $\mathbb{C} = \{a + b\mathrm{i} : a, b \in \mathbb{R}\}$, $\mathrm{i}^2 = -1 \cong \mathbb{R}[x]/(x^2 + 1)$ (exercise).

We'll use greek letters to denote complex numbers.

- $\mathbb{C}$ is a commutative ring with a 1 (in particular, an ID)
- $\mathbb{C}$ is a Field
- Conjugation $\alpha \mapsto \overline{\alpha}$ where $\overline{a + b\mathrm{i}} = a - b\mathrm{i}$
- Note that $\overline{\alpha\beta} = \overline{\alpha}\overline{\beta}$ and $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$, so conjugation is a ring homomorphism from $\mathbb{C} \to \mathbb{C}$.
- "Norm" function $N : \mathbb{C} \to \mathbb{R}, N(\alpha) = \alpha\overline{\alpha}$ so $N(a + b\mathrm{i}) = a^2 + b^2$
- $N(\alpha\beta) = N(\alpha)N(\beta)$

Definition 169. $\mathbb{Z}[\mathrm{i}] \subset \mathbb{C}$ is the subring $\{a + b\mathrm{i} : a, b \in \mathbb{Z}\}$. Called the Gaussian Integers.

Facts about $\mathbb{Z}[\mathrm{i}]$:

- It is a commutative ring with a 1
- It is an integral domain
- $(\mathbb{Z}[\mathrm{i}])^\times = \{\pm 1, \pm\mathrm{i}\}$ (the set of units)
  (Pf sketch: If u is a unit then $1 = N(1) = N(u^{-1}u) = N(u^{-1})N(u)$, then case)
- It is a Euclidean Domain with the norm N.

Proposition 170. $\mathbb{Z}[\mathrm{i}]$ *is a Euclidean Domain with the norm N.* $N(a + b\mathrm{i}) = a^2 + b^2$

Proof. Fix $\alpha, \beta \in \mathbb{Z}[\mathrm{i}]$ with $\beta \neq 0$. Want $\chi, \rho \in \mathbb{Z}[\mathrm{i}]$ such that $\alpha = \chi\beta + \rho$ and $N(\rho) < N(\beta)$ (or $\rho = 0$)
Let's look at all possible numbers $\{\chi\beta : \chi \in \mathbb{Z}[\mathrm{i}]\} = \mathbb{Z}[\mathrm{i}]\beta$.
If $\beta = a + b\mathrm{i}$, then $\mathrm{i}\beta = -b + a\mathrm{i}$. (In geometric terms, this equates to rotating the vector β 90° CCW)
$N(\alpha - \chi\beta) < N(\beta)$ So, $\alpha = \chi\beta + \rho$ □

Corollary 171. *Since* $\mathbb{Z}[\mathrm{i}]$ *is a Euclidean Domain, it is also a PID and a UFD, so the set of primes is equal to the set of irreducibles.*

Question: What are the irreducibles?
Let's try prime $p \in \mathbb{Z}$. $2 = (1 + \mathrm{i})(1 - \mathrm{i}), 5 = (2 + \mathrm{i})(2 - \mathrm{i}), 7$✓

Proposition 172. *If* $p \in \mathbb{Z}$ *is prime (in* $\mathbb{Z}$*) and* $p \equiv 3 \pmod 4$ *then* p *is still prime (irreducible) in* $\mathbb{Z}[\mathrm{i}]$.

Proof. Towards a contradiction, suppose that $p = \alpha\beta$ for non-units $\alpha, \beta \in \mathbb{Z}[\mathrm{i}]$.
$N(p) = p^2 = N(\alpha)N(\beta)$. Also, $N(\alpha), N(\beta) \neq 1$. So, $N(\alpha) = N(\beta) = p$. Say $\alpha = a + b\mathrm{i}$. So $p = N(\alpha) = a^2 + b^2$. Hence $a^2 + b^2 \cong 3 \pmod 4$, which is a contradiction. The remainder of the proof is homework. □

Next goal: show all other primes *are* reducible.

Proposition 173. *Suppose* p *is prime in* $\mathbb{Z}$, $p \equiv 1 \pmod 4$. *Then* $\exists n \in \mathbb{N}$ *such that* $n^2 \equiv -1 \pmod p$.

Proof. We work in the field $\mathbb{F} = (\mathbb{Z}/p\mathbb{Z}, +, \times)$ and the multiplicative group $G = (\mathbb{F} \setminus \{0\}, \times)$. So $|G| = p - 1 \equiv 0 \pmod 4$ So $4 = 2^2$ divides $|G|$ By Sylow, $\exists H \leq G$ with $|H| = 4$. So $\forall h \in H$, $|h| \in \{1, 2, 4\}$

Claim. If $g^2 = 1$ then $g = \pm 1$

Proof of claim. Fix such a g, work in $\mathbb{F}$. $(g + 1)(g - 1) = g^2 - 1 = 0$. Thus, $g = \pm 1$. □

Hence, $\exists h \in H$ of order 4 $h^2 \neq 1$ but $(h^2)^2 = h^4 = 1$. So $h^2 = -1$ in $\mathbb{F}$. Now fix $n \in \mathbb{N}$ such that $n \equiv h \pmod p$. Then $n^2 \equiv -1 \pmod p$. □

Proposition 174. *Suppose* p *is prime (in* $\mathbb{Z}$*) and* $p \equiv 1 \pmod 4$. *Then* p *is* not *prime (irreducible) in* $\mathbb{Z}[\mathrm{i}]$

Proof. Fix $n \in \mathbb{N}$ such that $n^2 \equiv -1 \pmod p$ (i.e., $p \mid (n^2 + 1)$). Factor $1 + n^2 = (1 + n\mathrm{i})(1 - n\mathrm{i})$ so $p \mid (1 + n\mathrm{i})(1 - n\mathrm{i})$ (in $\mathbb{Z}[\mathrm{i}]$). Suppose towards a contradiction that p is prime. Then p divides a factor. Say $p \mid (1 + n\mathrm{i})$.

Claim. $p|(1-n\mathrm{i})$ as well.

Proof. We know that $p = \overline{p}|\overline{(1+n\mathrm{i})} = (1-n\mathrm{i})$. □

Hence, $p|(1 \pm n\mathrm{i})$. So $p|(1+n\mathrm{i}) + (1-ni)$, so $p|2$, contradiction $(N(p) > N(2))$ □

Theorem 175 (Fermat)**.** *p prime, $p \equiv 1 \pmod 4$. Then, $\exists a, b \in \mathbb{N}$ such that $a^2 + b^2 = p$ and a, b are unique.*

Lecture 32 (2016–04–08).

Suppose R is an ID. When is $R[x]$ a UFD? It is when R is a field. If $R[x]$ is a UFD. R "$\subseteq$" $R[x]$ as constant polynomials. The units of $R[x]$ are the units of R. So $R[x]$ is a UFD $\implies$ R is a UFD.

Theorem 176. *If R is a UFD, so is $R[x]$.*

Corollary 177. *$\mathbb{Z}$ is a UFD, so $\mathbb{Z}[x]$ is a UFD. Also, $(\mathbb{Z}[x])[y] = \mathbb{Z}[x, y]$ is a UFD.*

Some basic facts about UFDs:
Fix UFD R with field of fractions F (Think $R = \mathbb{Z}, F = \mathbb{Q}$). Abuse notation and say $R \subseteq F$ with $r = \frac{r}{1}$.
Facts (when we say gcd = 1, we mean any unit):

(1) If $a, b \in R$ nonzero, then $\gcd(a, b)$ exists (collect common irreducible factors). Similarly, $\gcd(a, b, c) = \gcd(a, \gcd(b, c)) = \gcd(\gcd(a, b), c)$
(2) In the field of fractions F, we can represent an $f \in F$ as $\frac{a}{b}$ with $\gcd(a, b) = 1$.
(3) Given $f_1, \ldots, f_n \in F$ nonzero, can find $d \in R$ such that $\gcd(d, df_1, df_2, \ldots, df_n) = 1$ and each $df_1, \ldots, df_n \in R$ (d is the lowest common denominator).
(4) If $c|ab$ and $\gcd(a, c) = 1$ then $c|b$.

Example (Annoying example). $2x + 4$ is irreducible in $\mathbb{Q}[x]$.
But, $2x + 4$ is reducible in $\mathbb{Z}[x]$ as $2(x + 2)$ is a proper factorization (as 2 is not a unit in $\mathbb{Z}$)
Next, some definitions. Let $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$.

Definition 178. We define the content of f $c(f)$, to be $\gcd\{a_0, a_1, \ldots, a_n\}$.
For example, $c(2x + 4) = 2$

Definition 179. If $c(f) = 1$, we say f is primitive.

Lemma 180 (Gauss)**.** *If R is a UFD and $f, g \in R[x]$ are primitive, then fg is also primitive.*

Proof. Towards a contradiction, suppose $c(fg)$ is not a unit. Fix any irreducible $p \in R$ with $p|c(fg)$. Let $P = (p) = pR$. p irreducible $\implies$ p prime (because UFD). Thus P is a prime ideal. So, R/P is an ID, hence so too is $(R/P)[x]$.

Claim. If $\varphi : R \to S$ is a ring homomorphism, then $\psi : R[x] \to S[x]$ defined by $\psi(a_n x^n + \ldots + a_0) = \varphi(a_n)x^n + \ldots + \varphi(a_0)$

The proof is left to the reader.
Build $\psi : R[x] \to (R/P)[x]$ by $\psi(a_n x^n + \ldots + a_n) = (a_n + P)x^n + \ldots + (a_0 + P)$. By the previous claim, ψ is a ring homomorphism. Note $\psi(f)\psi(g) = \psi(fg) = (0 + P)$ (the constant zero polynomial in $(R/P)[x]$).
Thus, $\psi(f) = 0 + P$ or $\psi(g) = 0 + P$ If $\psi(f) = 0$, then $p|c(f)$ contradicts f being primitive. The same argument applies to g. □(Lem.)

Corollary 181. *For $f, g \in R[x]$, $c(fg) = c(f)c(g)$.*

Proof. Fix primitive $f_0, g_0 \in R[x]$ such that $f = c(f)f_0$ and $g = c(g)g_0$.
Then,

$$fg = c(f)f_0c(g)g_0 = \underbrace{c(f)c(g)}_{\in R} \cdot \underbrace{f_0g_0}_{\substack{\in R[x] \\ \text{primitive}}}$$

□(Cor.)

Proposition 182. *If $f \in R[x]$ is primitive, f is reducible in $R[x]$ iff f is reducible in $F[x]$.*

Proof. $R[x]$ reducible $\implies$ $F[x]$ reducible.

If $f(x) = g(x)h(x)$ is a proper factorization in $R[x]$. Then neither g nor h is constant. So, both have degree at least 1. Thus, neither is a unit in $F[x]$.

$F[x]$ reducible $\implies$ $R[x]$ reducible.

If $f(x) = g(x)h(x)$ is a proper factorization in $F[x]$. We may take $\tilde{g}, \tilde{h} \in R[x]$ such that $f = \tilde{g}\tilde{h}$ and $g \sim \tilde{g}$ and $h \sim \tilde{h}$ in $F[x]$

The remainder of the proof will be typed up soon.

□

Index